Review Article

Phishing Detection: Analysis of Visual Similarity Based Approaches

Ankit Kumar Jain and B. B. Gupta

National Institute of Technology, Kurukshetra, India

Correspondence should be addressed to B. B. Gupta; gupta.brij@gmail.com

Phishing is one of the major problems faced by cyber-world and leads to financial losses for both industries and individuals. Detection of phishing attack with high accuracy has always been a challenging issue. At present, visual similarities based techniques are very useful for detecting phishing websites efficiently. Phishing website looks very similar in appearance to its corresponding legitimate website to deceive users into believing that they are browsing the correct website. Visual similarity based phishing detection techniques utilise the feature set like text content, text format, HTML tags, Cascading Style Sheet (CSS), image, and so forth, to make the decision. These approaches compare the suspicious website with the corresponding legitimate website by using various features and if the similarity is greater than the predefined threshold value then it is declared phishing. This paper presents a comprehensive analysis of phishing attacks, their exploitation, some of the recent visual similarity based approaches for phishing detection, and its comparative study. Our survey provides a better understanding of the problem, current solution space, and scope of future research to deal with phishing attacks efficiently using visual similarity based approaches.

1. Introduction

Phishing is a crime in which a perpetrator sends the fake e-mail, which appears to come from popular and trusted brand or organization, asking to input personal credential like bank password, username, phone number, address, credit card details, and so forth [1–4]. The fake e-mails often look amazingly legitimate, and even the website where the Internet user is asked to input personal information also looks similar to legitimate one. Phishing messages propagate over e-mail, SMS, instant messengers, social networking sites, VoIP, and so forth, but e-mail is the popular way to perform this attack and 65% of the total phishing attack is achieved by visiting the hyperlink attached to the e-mail [5]. Moreover, spear phishing attack is becoming popular nowadays. Business e-mail compromise (BEC) is observed as a major Internet threat in 2015 [6]. In BEC, the intruder uses spear phishing methods to fool organizations and Internet persons. More sophisticated spear phishing attacks [7–9] targeted particular individual or groups within the organization. Phishing is metaphorically similar to fishing in the water, but instead of trying to catch a fish, attackers try to steal consumer's personal information [10, 11]. When a user opens a fake webpage and enters the username and protected password, the credentials of the user are acquired by the attacker which can be used for malicious purposes [12–22]. Phishing websites look very similar in appearance to their corresponding legitimate websites to attract large number of Internet users. Recent developments in phishing detection have led to the growth of numerous new visual similarity based approaches. Visual similarity based approaches compare the visual appearance of the suspicious website to its corresponding legitimate website by using various parameters. Due to different phases of phishing detection, this paper contains the following:

(i) Background, History, and Statistics section presents the history of phishing attacks, worldwide financial losses due to phishing attacks, the lifecycle of phishing attack, and classification of various types of phishing attacks. This section describes the overall picture of phishing attacks from a high level perspective.

(ii) Next, we describe how attacker fools an Internet user and how they bypass the antiphishing system.

(iii) Similarly, we present various types of phishing detection techniques, their advantages, and drawbacks.

(iv) Also, we provide a comprehensive literature review of visual similarity based phishing detection approaches, which incorporates document object model (DOM), Cascading Style Sheet (CSS), HTML tag, image processing, and hybrid techniques. Moreover, we present a comparison between various visual similarity based antiphishing techniques. It provides a better understanding of the problem, current solution space, and future research scope to efficiently deal with phishing attacks using visual similarity based approach.

(v) In addition, we provide several issues and challenges in detection of phishing attacks.

The rest of the paper is structured as follows. Section 2 contains the background, history, and statistics of phishing attack. Section 3 describes the overview of phishing detection using visual similarity based approaches. Section 4 presents the taxonomy of various types of phishing detection and filtering techniques; especially this section focuses on visual similarity approaches in detail. Section 5 presents the performance and evaluation matrices to judge the antiphishing system. Section 6 presents the open issues and challenges in phishing detection and protection. Finally, Section 7 concludes the paper.

2. Background, History, and Statistics

A phishing scam has attracted the attention of both academicians and corporate researchers as it is a serious privacy and web security threat [23–33]. Phishing cannot be controlled by firewalls or any encryption software [34–36].

2.1. Brief History. First phishing attack was observed on America online network systems (AOL) in the early 1990s [37] where many fraudulent users registered on AOL website with fake credit card details. AOL passed these fake accounts with a simple validity test without verifying the legitimacy of the credit card. After activation of the fake account, attackers accessed the resources of America online system. At the time of billing, AOL determined that the accounts were fraudulent, and associated credit cards were also not valid; therefore AOL ceased these accounts immediately. After this incident, AOL took measures to prevent this type of attack by verifying the authenticity of credit card and associated billing identity, which also enabled the attackers to change their way of obtaining AOL accounts. Instead of creating a fake account, attackers would steal the personal information of registered AOL user. Attackers contacted registered AOL users through instant messenger or e-mail and asked them to verify the password for security purposes. E-mail and instant messages appeared to come from an AOL employee. Many users provided their passwords and other personal information to the attackers. The attackers then used
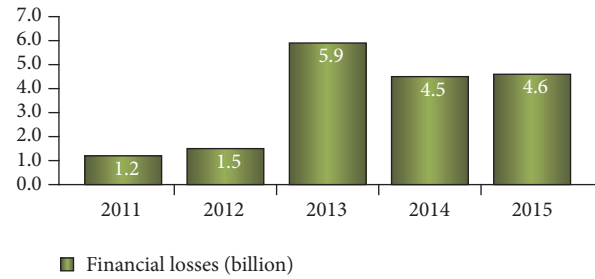

Figure 1: Worldwide financial losses (in billion) due to phishing attack.

the variously billed portions of America online website on behalf of a legitimate user. Moreover, an attacker no longer restricts themselves to masquerading America online website but actively masquerade a large number of financial and electronic commerce websites.

2.2. Statistics. According to Internet world stats [38], total numbers of Internet users worldwide are 2.97 billion in 2014; that is, more than 38% of the world population uses Internet. Hackers take advantage of the insecure Internet system and can fool unaware users to fall for phishing scams. Phishing e-mail is used to defraud both individuals and financial organizations on the Internet. The Anti-Phishing Working Group (APWG) [39] is an international consortium which is dedicated to promoting research, education, and law enforcement to eliminate online fraud and cyber-crime.

In 2012, total phishing attack increased by 160% over 2011, signifying a record year in phishing volumes. The total phishing attacks detected in 2013 were approximately 450000 and led to financial losses more than 5.9 billion dollars [39]. Total attack increases by 1% in 2013 as compared to 2012. The total number of phishing attacks noticed in Q1 (first quarter) of 2014 was 125,215, a 10.7 percent increase over Q4 (fourth quarter) of 2013. More than 55% of phishing websites contain the name of the target site in some form to fool users and 99.4% of phishing websites use port 80 [40]. According to the APWG report in the first quarter of 2014, second highest number of phishing attacks ever recorded was between January and March 2014 [40] and payment services are the most targeted industry. During the second half of 2014, 123,972 unique phishing attacks were observed [41]. In the year 2011, total financial losses were 1.2 billion, and they rose to 5.9 billion dollars in 2013. The financial losses due to phishing attack in 2014 and 2015 were 4.5 and 4.6, respectively, as shown in Figure 1 [42]. The growth of phishing attacks from 2005 to 2015 is shown in Figure 2.

2.3. Phishing Mechanism. The phishing mechanism is shown in Figure 3. The fake website is the clone of targeted genuine website, and it always contains some input fields (e.g., text box). When the user submits his/her personal details, the
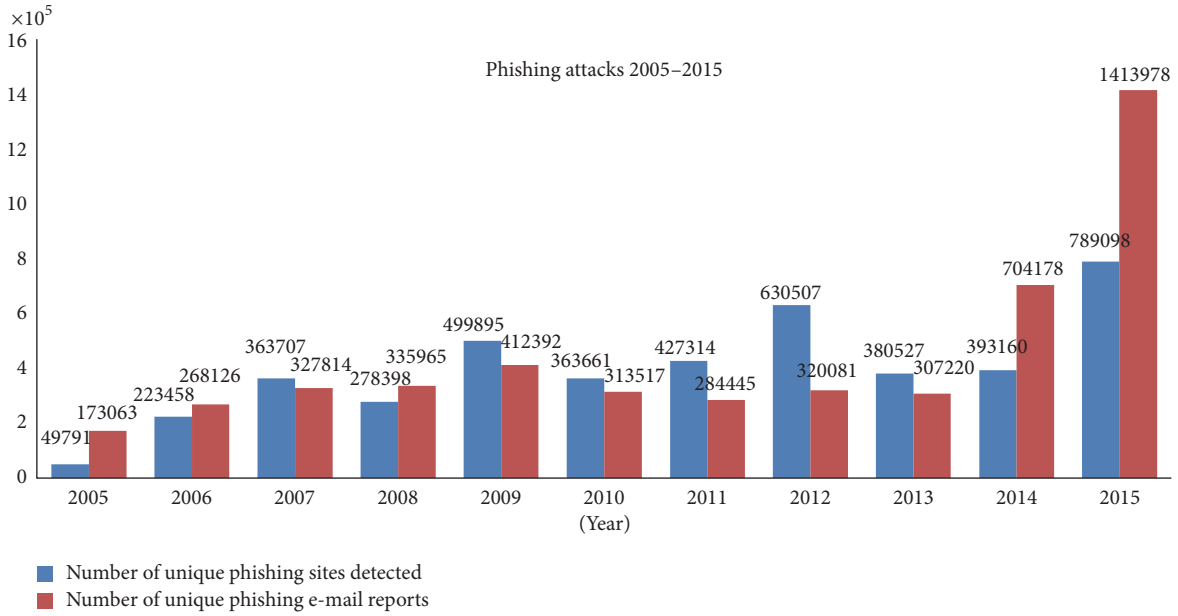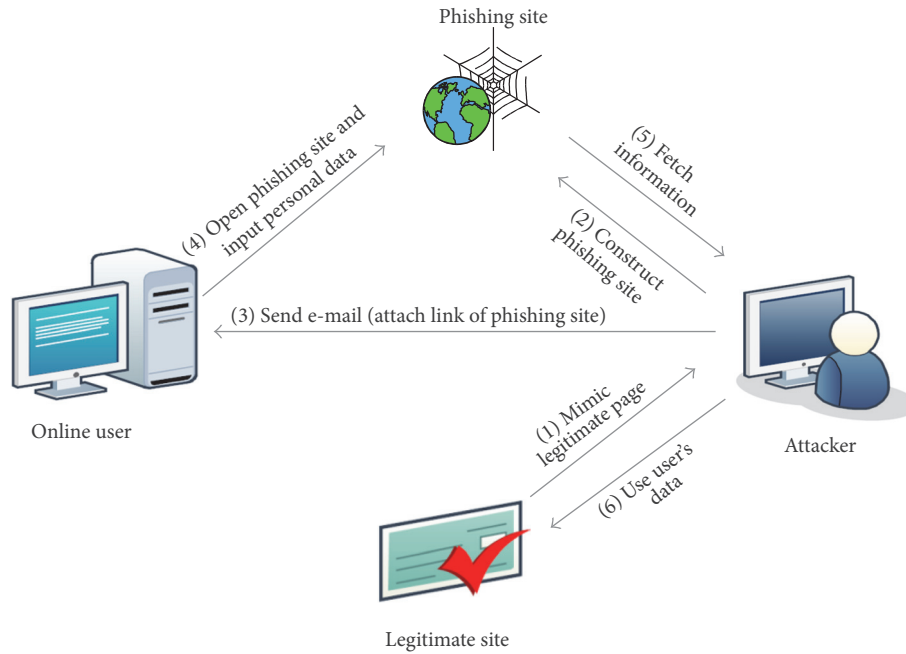
Figure 2: Phishing growth by 2005–2015.

Figure 3: Phishing mechanism.

information is transferred to the attacker. An attacker steals the credential of the innocent user by performing following steps:

Construction of Phishing Site. In the first step attacker identifies the target as a well-known organization. Afterward, attacker collects the detailed information about the organization by visiting their website. The attacker then uses this information to construct the fake website.

URL Sending. In this step, attacker composes a bogus e-mail and sends it to the thousands of users. Attacker attached the URL of the fake website in the bogus e-mail. In the case of spear phishing attack, an attacker sends the e-mail to selected users. An attacker can also spread the link of phishing website with the help of blogs, forum, and so forth [43].

Stealing of the Credentials. When user clicks on attached URL, consequently, fake site is opened in the web browser. The
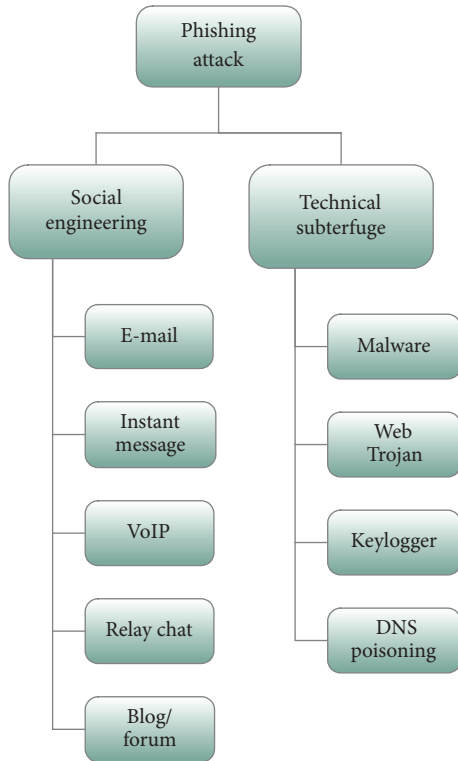
Figure 4: Types of phishing attack.

fake website contains a fake login form which is used to take the credential of an innocent user. Furthermore, attacker can access the information filled by the user.

Identity Theft. Attacker uses this credential of malicious purposes. For example, attacker purchases something by using credit card details of the user.

2.4. Taxonomy of Phishing Attack. Attacker performed the phishing attack by utilising the technical subterfuge and social engineering techniques [40, 44]. In social engineering techniques, attackers carry out this attack by sending bogus e-mail. Attackers often convince recipients to respond using names of banks, credit card companies, e-retailers, and so forth [45]. Technical subterfuge strategies install malware into user's system to steal credentials directly using Trojan and keylogger spyware [46]. The malware also misaddresses users to fake websites or proxy servers. Attackers attached malware or embedded malicious links in the fraudulent e-mails and when the user opens the fraud hyperlink, malicious software is installed on the user's system, which collected the confidential information from the system and sent it to the attacker (e.g., keylogger software sends the details of every key hit by the user). Attackers may also get remote access to victim's computer and collect data whenever attackers want. In this paper, we focus on social engineering schemes, as it is the most popular way to steal victim's information by phishing. Classification of various phishing attacks is shown in Figure 4.

2.5. Antiphishing Technique: Modus Operandi. A phishing scam starts with spreading bogus e-mail. After receiving an e-mail, antiphishing techniques start working, either by redirecting the phishing mail in the spam folder or by showing a warning when an online user clicks on the link of phishing URL. The lifecycle of phishing attack is shown in Figure 5. The following steps are involved in phishing lifecycle:

Step 1. Attacker creates the fake copy of a popular organization and sends the URL of fake website to the large number of Internet users using e-mail, blog, social networking sites, and so forth.

Step 2. In the case of fake e-mail, every e-mail is first to pass through the DNS-based blacklist filters. If the domain is found in the blacklist, then e-mail is blocked before it reached to SMTP mail server. There are also various solutions available which block the fake e-mail based on structural features of mail [44].

Step 3. If a fake e-mail bypasses the blacklist and features based solutions and if the user opens attached link in the e-mail then some browser based blacklist techniques block the site at client side.

Step 4. Some other solutions like the heuristic and visual similarities based approaches also blocked the webpage only when the browser requests for any suspicious webpage.

Step 5. If the phishing attack bypasses all the solutions then it steals the credential of innocent users and sends it to the attacker. The attacker uses this information for financial or some other benefits.

3. Visual Similarity Based Phishing Detection and Filtering Approaches

A user could become the victim of the phishing attack by looking the high visual resemblance of phishing website with the targeted legitimate site, such as page layouts, images, text content, font size, and font colour. The fake and genuine webpages of PayPal are shown in Figure 6, and both pages have same visual appearance but different URLs. It is not always necessary that the people carefully notice on URL and SSL (Secure Socket Layer) certificate of websites. If an attacker does not copy the visual appearance of targeted website well, then chances of inputting credentials by Internet users are very less. An attacker fools the user by the following ways:

(1) *Visual Appearance.* The phishing website looks similar to its legitimate website. Attackers used to copy the HTML source code of genuine website to build the fake website.

(2) *Address Bar.* Attackers also cover the address or URL bar of website by script or image. The user would believe that they are inputting information on the right website.
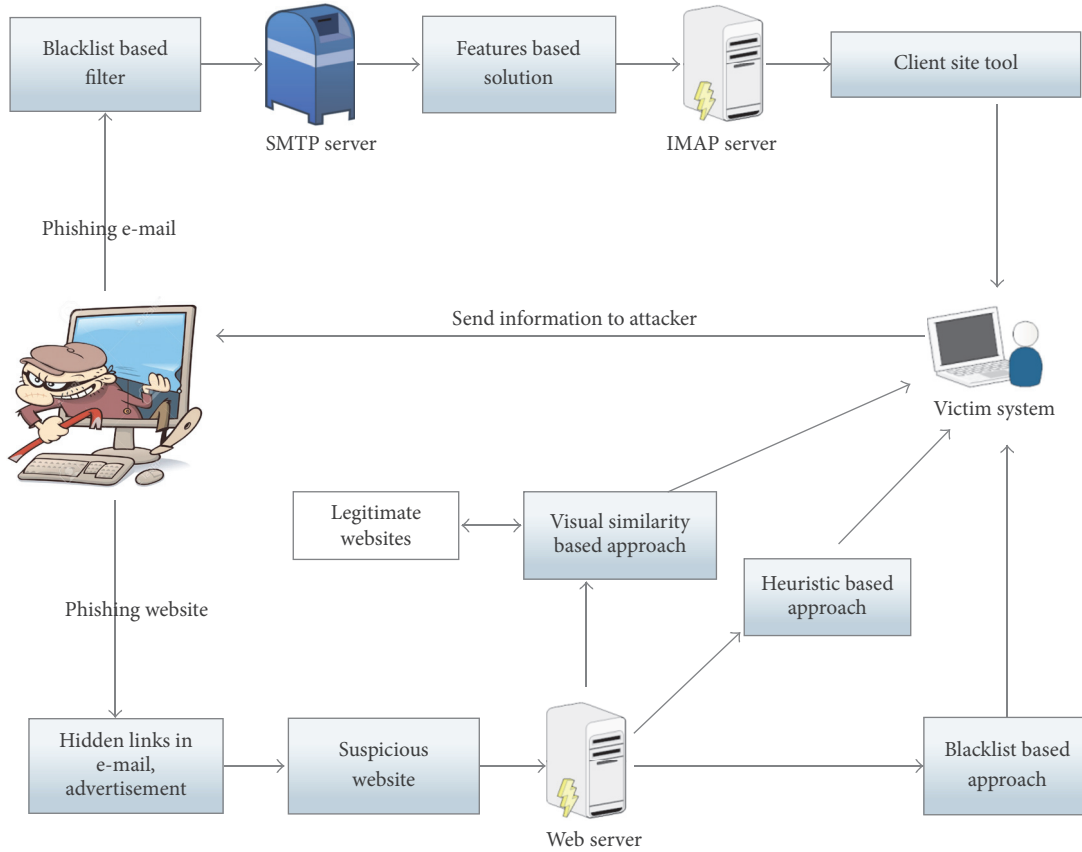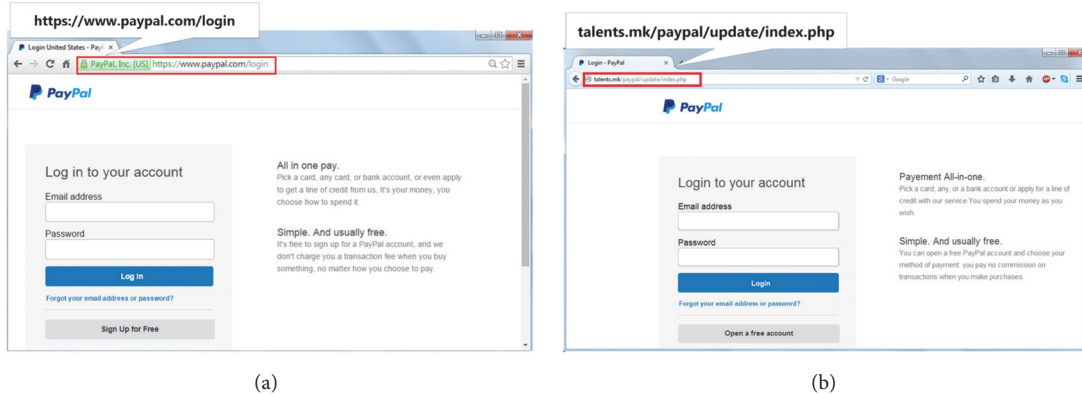
Figure 5: Life cycle of phishing attack.

(a)

(b)

Figure 6: (a) Legitimate PayPal webpage and (b) phishing webpage of PayPal.

(3) *Embedded Objects*. Attackers use embedded objects (images, scripts, etc.) to hide the textual content and HTML coding from the phishing detection approaches.

(4) *Favicon Similarity*. Favicon is an image icon associated with the particular website. An attacker may copy the favicon of targeted website. If the favicon shown in the address bar is other than the current website, then it is considered as a phishing attempt.

Dhamija et al. [47] conducted a survey on various participants to identify whether a website is phishing or genuine. Participants were unable to identify 90% of phishing sites. Many participants wrongly judged the site on the basis of their text content and visual appearance. They also found that even an experienced user could also be fooled by the visual appearance of a fake website, and 23% of the users do not look at the address bar of a website. Therefore, we can say that if the appearance of a phishing site is similar to its legitimate one

and domain is different then also users can easily be trapped by the attackers.

3.1. Advantages of Visual Similarity Approach. There are two major techniques for phishing detection: the first is the list-based (blacklist or white list) and the other is heuristic based approaches [3, 49, 50]. In the blacklist based methods, the suspicious domain is matched with some predefined stored phishing domains which are blacklisted [51–53]. The negative aspect of this scheme is that blacklist usually does not cover all phishing websites because a newly launched fraud website takes the substantial amount of time to get added in the blacklist record. In addition, 47% to 83% of fake URLs updated in the blacklist after twelve hours [51]. Heuristic based approaches match the heuristic design of the website with predefined rules. However, attackers can forge such features. Heuristic based approaches detect the phishing webpage by matching the features like the keywords, IP address, URL features, popup windows, SSL certificates, external hyperlinks, and so forth. Sometimes attacker also constructs a website in such a manner that the features are not matched with the predefined list of features. As we see some heuristic based approaches have high false positive rate [29, 54–57]. The following are the two primary advantages of visual similarity based approaches.

(1) In order to avoid phishing detection technique, attackers usually insert images, Flash, ActiveX, and Java Applet in place of HTML text. Visual similarity based detection approaches can quickly detect such embedded objects present in phishing webpage.

(2) Visual similarity based techniques use a signature to identify phishing webpages. The signature is created by taking common features from the whole website rather than a single webpage. Therefore, one signature is sufficient to detect various targeted webpages of a single website or different versions of a website.

4. Taxonomy of Phishing Detection and Filtering Based on Visual Similarity

A variety of detection approaches against phishing attack has been proposed in the literature. Phishing detection techniques are widely divided into two classes. First is based on user education, and the other is based on software. Software based techniques are further categorized into machine learning [58–60], blacklist [61, 62], and visual similarity based approaches. Blacklist based approaches keep a list of phishing URLs. Updating the newly launched phishing websites in the blacklist in time constraint manner is a difficult task. A heuristic based approach utilises standard features of phishing websites, such as the login form, URL, and web traffic, to take appropriate decision [63, 64]. When attacker designs a new phishing website, they always consider the heuristic characteristic to bypass the phishing detection system.

We can broadly classify the visual similarity based approaches into HTML document object model (DOM) tree, visual features, Cascading Style Sheet (CSS) similarity, pixel based, visual perception, and hybrid approaches as mentioned in Figure 7. The detailed descriptions of visual similarity based approaches are explained in the following subsections.

4.1. Document Object Model. Document object model (DOM) is a language independent and multiplatform convention for demonstrating objects in XML, XHTML, and HTML documents. DOM represents the logical structure of documents and the way of a document is addressed and controlled. In this model, the document is represented in the form of the tree, so it is called DOM tree as shown in Figure 8. In the DOM based phishing detection system, the DOM tree of the suspicious webpage is compared with the legitimate webpage as the attackers always try to mimic the original legitimate webpage and the page layout is expected to be similar.

Rosiello et al. [48] presented an approach based on the reuse of same information on multiple websites. In the proposed approach, if a user reuses the same information (i.e., same user name, password, etc.) on multiple websites, then the system generates a warning. The system compares the document object model (DOM) tree of the first webpage where the data was initially entered and another webpage, where the data is reused. If the DOM tree between these two webpages is found to be similar, then the system is considered as a phishing attack or else, the system find legal reuse of information as depicted in Figure 9. The proposed approach maintains a list of previously visited websites and the information filled in their forms to compare with the current website information. The negative aspect of this approach is that it only compares the new webpage with the only previously visited webpages.

The document object model of a webpage is represented by a tree. A tree is a type of graph $G(V, E)$, where there is only one path between any two vertices. Vertices represent the tags, and edges represent the hierarchy between the tags.

Two DOM trees, $T(V, E)$ and $T'(V', E')$, are equivalent if they satisfy the following properties:

(i) Values of the corresponding vertices are the same.

(ii) Indices of matching edges are the same.

(iii) Both trees are isomorphic [65].

The layout similarity of the legitimate and the suspicious webpages is determined by the ratio of the weighted number of matched vertices to the total vertices in the legitimate webpage, as shown by

$$\text{Layout Similarity} = \sum_{n=1}^{n=k} \frac{W(V_n)}{V_n}, \tag{1}$$

where V_n represents the nth vertices and k represent the total vertices in the legitimate webpage. W is the weight function, which assigns similarity score between 0 and 1 for
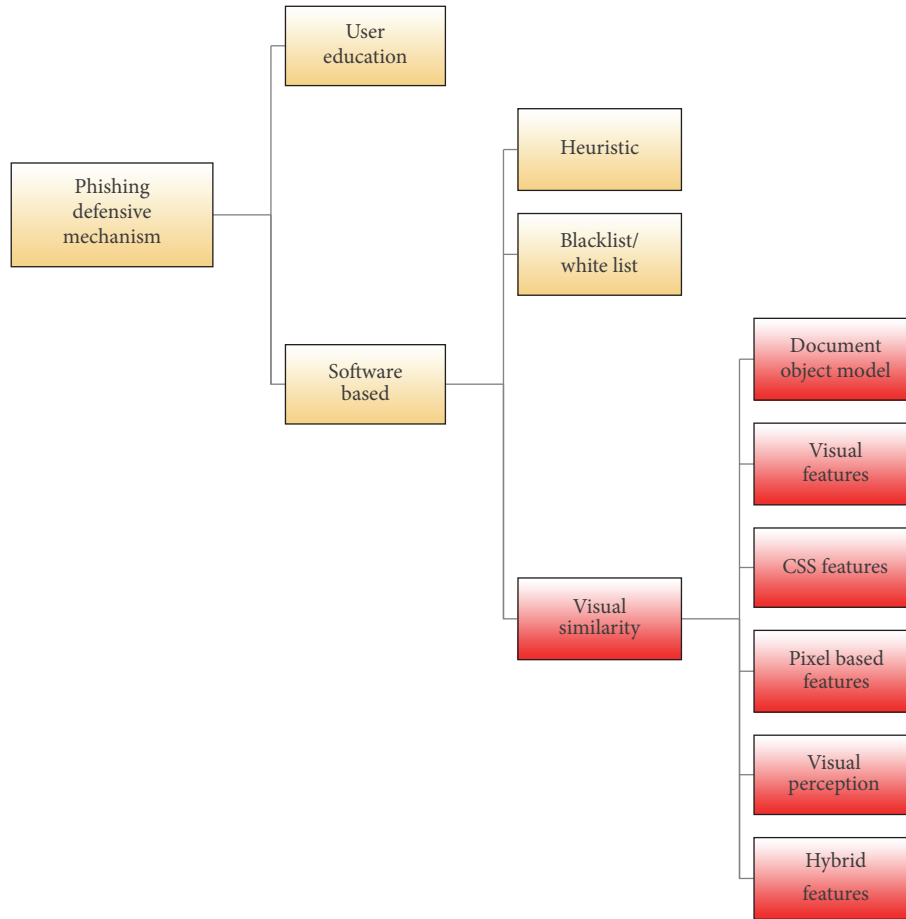
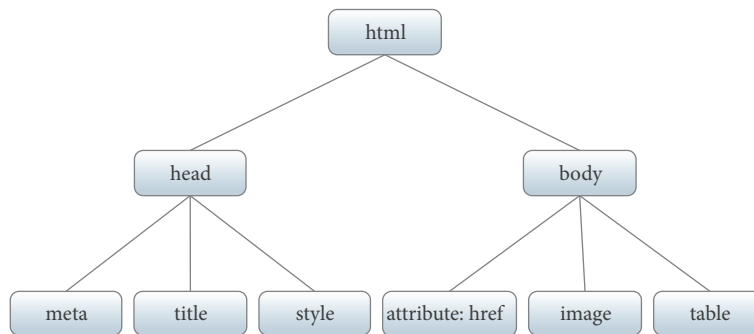FIGURE 7: Overview of phishing defensive mechanism.

FIGURE 8: DOM tree.

two vertices. If the layout similarity is greater than a given threshold, then webpages are called similar.

4.2. Visual Features. There are two types of visual features: the first is the text content, and the other is the text features based like font colour, font size, background colour, font family, and so forth. Visual features based approaches match the visual features between different websites since most of the time

attacker copies the page content from the actual website. We discuss the visual features based solutions in the following subsections. Visual features which are used to compare the websites are shown in Table 1 [66].

4.2.1. Visual Similarity Assessment. Liu et al. [66] proposed an approach which contains the two modules. The first module detects the suspicious URLs and keywords at local e-mail
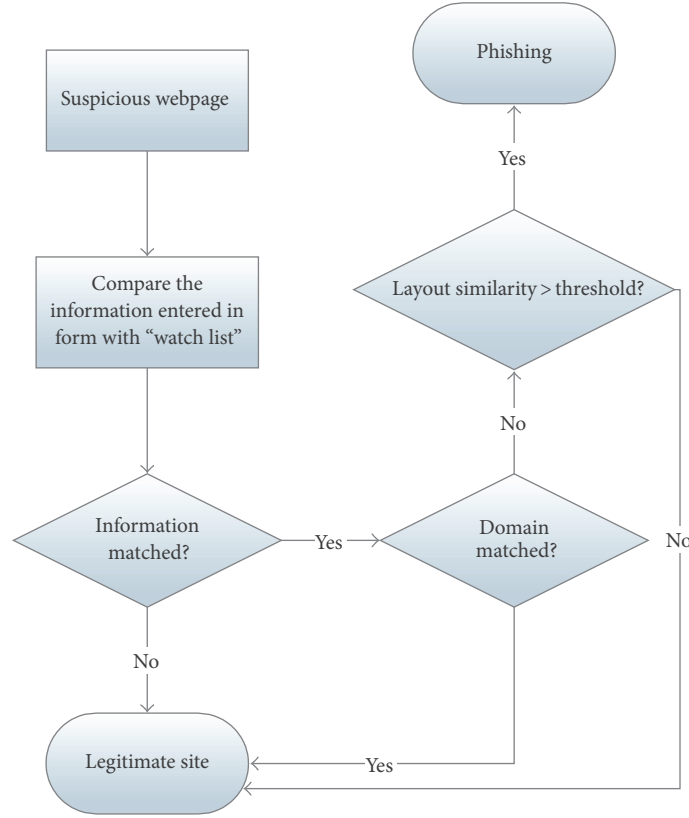
FIGURE 9: Flow chart of DOM based comparison [48].

server. After detection of the suspicious keywords or URLs in the e-mail, the second module compares the block level, layout, and style similarity for the suspicious webpage. The architecture of the proposed approach is shown in Figure 10.

(i) *Block Level*. The suspicious webpage is divided into blocks, for each block the visual features (features explained in Table 1) are extracted and matched with the corresponding legitimate webpage, and then the system calculates block level resemblance by the weighted average of matching blocks.

(ii) *Layout Level*. Layout similarity is calculated by dividing the total number of matched blocks to the total block present in the legitimate webpage.

(iii) *Overall Style*. Style similarity is calculated by taking histogram of each webpage's style feature. When similarity between the given and the legitimate webpage is greater than some predefined threshold, then the system marks the given webpage as a phishing webpage.

4.2.2. Site Signatures. Huang et al. [67] proposed a technique which creates unique web-based signature to identify the legitimate websites. Site signature is created by using the text (keywords) and images of the website. When a user opens a new webpage, the system matches the signature of presently

TABLE 1: Visual features of webpage.

Features name	Description and possible values
Text content	Text in a paragraph
Background colour	Background colour of text
Foreground colour	Foreground colour of text
Border colour	Border colour of webpage
Background image	Background image existing in webpage
Border line	Solid, dotted, and so forth
Border line thickness	Thickness of the border line
Font family	Calibri, arial, cambria, and so forth
Font colour	Black, blue, red, and so forth
Font size	Large, medium, small, and so forth
Text alignment	Left, center, right, and justify
Text style	Bold, underline, and so forth
Navigation (hyperlinks)	Values of hyperlinks
Image features	Height, width, src attributes, image position, and so forth
Image position	Position of image in webpage

opened webpage with stored signature in the database. If the signature matches but the domain name is different,
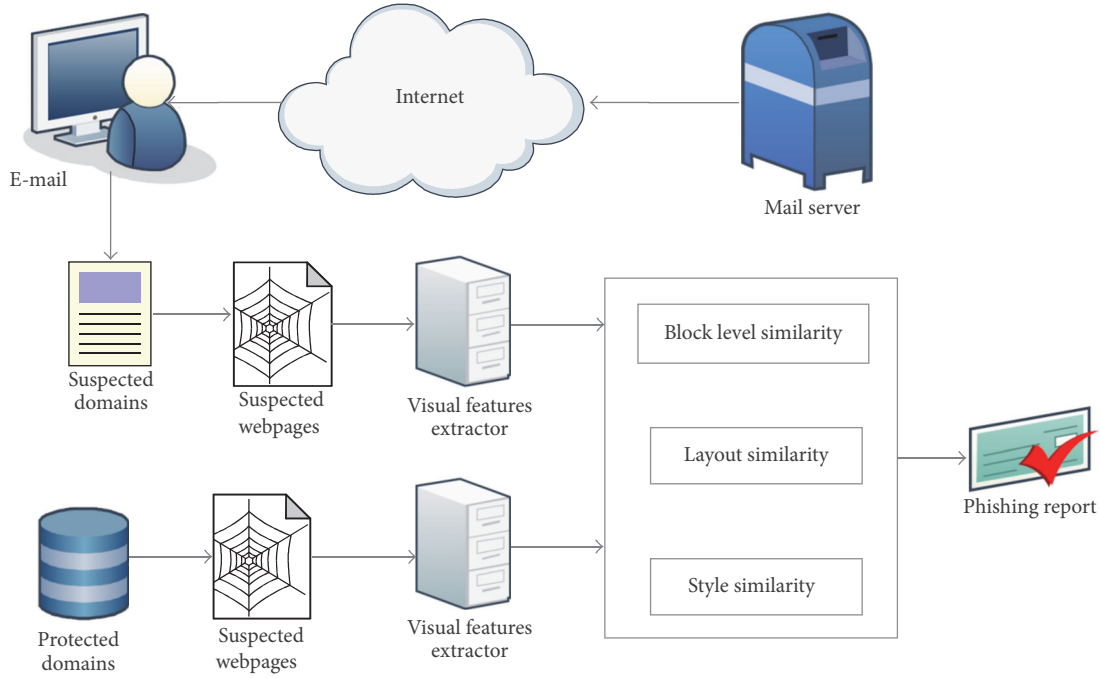
FIGURE 10: Architecture of visual similarity assessment [66].

then the webpage is declared phishing. The following are the properties of the proposed approach:

(i) The system uses text and image features to construct a unique signature for a website. Text features include the title keywords, URL keywords, and most frequent keywords using term frequency inverse domain frequency (TF-IDF) algorithm. Images are extracted from the home page as well as all the webpages associated with the home page through the hyperlinks.

(ii) Signature is created by extracting features from the entire website rather than a single webpage. Therefore, only one signature is enough to detect various targeted fake webpages of a website.

(iii) Signature uses the standard features of an entire website so this technique can also detect a phishing webpage which is partially copied from a legitimate website.

(iv) Signature is created using both image and text features. So, if an attacker uses only images in the fake webpage, the proposed approach can detect this type of attack.

The proposed technique initially creates signature for the newly visited website and matches it with stored signature. If a user visits a website for the first time and their corresponding legitimate site is not present (i.e., signature not matched with any stored signature) then the system creates signature and stores it in the database.

4.2.3. PhishZoo. Afroz and Greenstadt [68] proposed an antiphishing solution which creates the unique profile for a

website using URL, text contents, images (specially website logo), Secure Socket Layer (SSL) certificate, and scripts. PhishZoo matches the profile of the new site with the stored profiles in the database. PhishZoo stored the list of legitimate sites and their profiles in the profile database. In the first phase, PhishZoo only matches URL and SSL certificate with the stored profiles. If URL and SSL certificate match, then PhishZoo declares the website a legitimate or else the text content of the webpage is compared with the stored profiles. Architecture of PhishZoo is shown in Figure 11.

The following is the silent characteristic of PhishZoo:

(i) This approach matches the URL, SSL certificates, and webpage contents, which is an advantage over blacklist based approaches.

The comparison of various visual features based approaches (discussed in Section 4.2) on different attacks is presented in Table 2.

4.3. CSS Similarity. Cascading Style Sheets (CSS) is a language used for depicting the formatting of a document and setting the visual appearance of a webpage written in the HTML, XHTML, and XML. CSS is used to design the webpage content like fonts, colours, and page layout.

4.3.1. BaitAlarm. Mao et al. [71] proposed an algorithm to compare the CSS similarity between suspicious and legitimate website. The technique uses the CSS similarity concept because without using the same CSS, it is tough to achieve the same design as that of a legitimate site. CSS contains a list
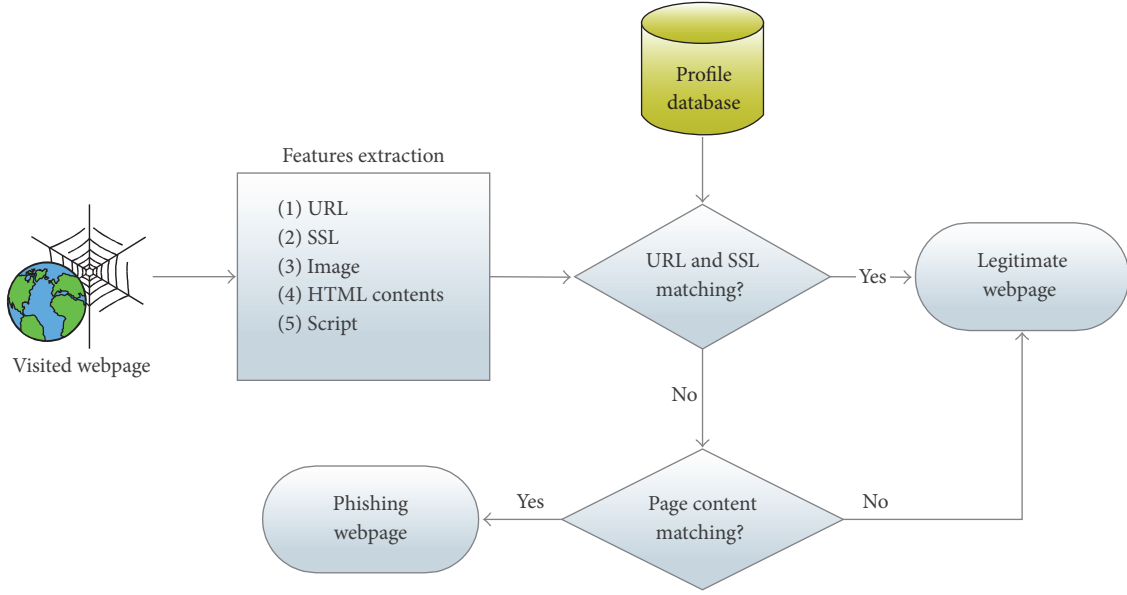
FIGURE 11: Architecture of PhishZoo [68].

TABLE 2: Comparison of visual features based approaches.

Approach	Zero-hour protection	Embedded object	Language independence	Partially copied webpage	DNS attack
Visual signature [66]	No	No	No	No	No
Site signature [67]	No	Yes	No	Yes	No
PhishZoo [68]	No	Yes	Yes	Yes	No

of rules, which relate a group of selectors, properties, and values to a set of declarations. Selectors can be divided into various categories, such as class selectors, tag selectors, id selectors, and some attribute selectors. Properties illustrate the attributes related to the elements that are selected by the selectors. For example, any tag contains colour, margin, font size, font family, padding properties, border, and values associated with each of these properties. The similarity of two CSS can be determined by extracting selectors, properties, and values. In addition to this approach, Mishra and Gupta [69] presented a hybrid solution based on URI and CSS matching. In this, the CSS matching is borrowed from the BaitAlarm. Algorithm 1 is used to compare CSS between two webpages [69].

The correct threshold to compare CSS between webpages can be calculated only after the experiment. This approach can also detect embedded noise contents like an image in a webpage which is used to sustain the visual similarity of the webpage.

4.4. Pixel Based Techniques. Pixel or image processing based approaches use the image processing applications to check the similarity between two webpages. Image processing based methods either take the screenshot or extract images from the suspicious webpage and compare the images against the legitimate webpage. These approaches believe that the two different websites of the different organizations cannot be similar. If the two images of different sites are similar, and their URLs are different, then one website is considered as phishing (shown in Figure 12).

4.4.1. Discriminative Keypoint Features. Chen et al. [72] proposed an antiphishing approach based on discriminative keypoint features. This approach considers detection of phishing webpage as an image matching problem. There are two modules in the proposed system. In the first module, the system takes the snapshot of suspicious webpage and captures invariant information around discriminative keypoints using Contrast Context Histogram (CCH). In the second module, the system calculates the similarity score between two pages based on the matching CCH descriptor. Verified authenticated webpages are stored in a local database.

To find out whether two images are identical, proposed approach fetches the vector of significant features from each image and compute the distance between those vectors. Moreover, the system measures this distance as the degree of

```
(1)  Fetch style sheet from suspicious website
(2)  Fetch style sheet of legitimate website
(3)  for each elements of suspicious website
(4)     for each element legitimate website
(5)        for each Selector_sus
(6)              If (Tag_sus == Tag_leg[i]) then tag++
(7)              If (Clas_sus == Class_leg[i]) then class++
(8)              If (ID_sus == ID_leg[i]) then id++
(9)              If (Other_sus == Other_leg[i]) then other++
(10)             Selector = max(Selector_suspicious, Selector_legitimate[i])
(11)       end for
(12)    end for
(13) end for
(14) CSS_Score = tag + class + id + otherSelector
(15) if (CSS_Score > CSS_threshold) then "URL is phishing"
(16) else "URL is Innocent"
(17) end if
```

ALGORITHM 1: Algorithm to compare CSS between two pages (suspicious and legitimate) [69].

visual difference between two images. If attackers replace the text content with the image, then this technique can detect it.

4.4.2. Goldphish. Dunlop et al. [73] proposed a browser based plug-in goldphish to identify phishing websites. Goldphish makes use of website logo to identify the fake website because the attacker can use the real logo of the targeted website to trap Internet users. It has the three stages:

(i) *Logo Extraction.* Goldphish extracts the website logo from the suspicious website and then converts it into text using optical character recognition (OCR) software.

(ii) *Legitimate Websites Extraction.* The text is used as a query for the search engine. To check the legitimacy of website, Goldphish uses trusted search engine "Google" because it always returns genuine websites in their top results.

(iii) *Comparison.* Suspicious website is compared with the top results obtained from search engine. If any of domain matched with the current website, then declare it a legitimate or otherwise make it a phishing site.

Goldphish can quickly identify the fake websites of popular organizations. However, the accuracy of the system depends on the OCR software. Goldphish also protects the users from "zero-hour" phishing attack.

4.4.3. Dynamic Watermarking. Singh et al. [74] used the dynamic watermarking technique to protect users at client side and defend against the man in the middle of attack. The proposed technique required extra information at the time of registration on a website like the secret key, watermark image, and its position. In this technique, the user identifies the legitimacy of a website by checking a unique image

and its position. Proposed technique has the three primary components:

(1) *Registration.* Whenever a user registers on a website for the first time, generally a website required credential of the user like username, password, and so forth. Moreover, in this technique user has to put three more fields: watermark image, its position, and secret key. Secret key acts as a primary key for the database.

(2) *Login Verification.* When the user opens the website after the registration, he/she has to verify the credential. In the login verification process, user has to enter correct secret key. If the website shows the correct watermarked image and its position (same as entered at the time of registration), then the website is legitimate.

(3) *Closing.* User only needs to know the watermark image and its position. At the time of logout, the user can change a new watermark image and position.

4.4.4. Image Layout Analysis Based Approach. Lam et al. [75] proposed an approach to detect phishing website by matching pixels to compute the similarity degree between websites. Otsu's threshold method [76] is used to convert the webpage into black-and-white images and then analyse the pixels of the images. Proposed approach divides the image into nonoverlapping layout blocks and compares these blocks between two webpages. Layout block is the primary element for building a webpage as shown by rectangle blocks in Figure 13. Algorithm of matching layout block between webpages is explained as follows:

Block Matching. Suspicious webpage X contains the blocks $x_1, x_2, x_3, \ldots, x_n$ and legitimate webpage Y contains the
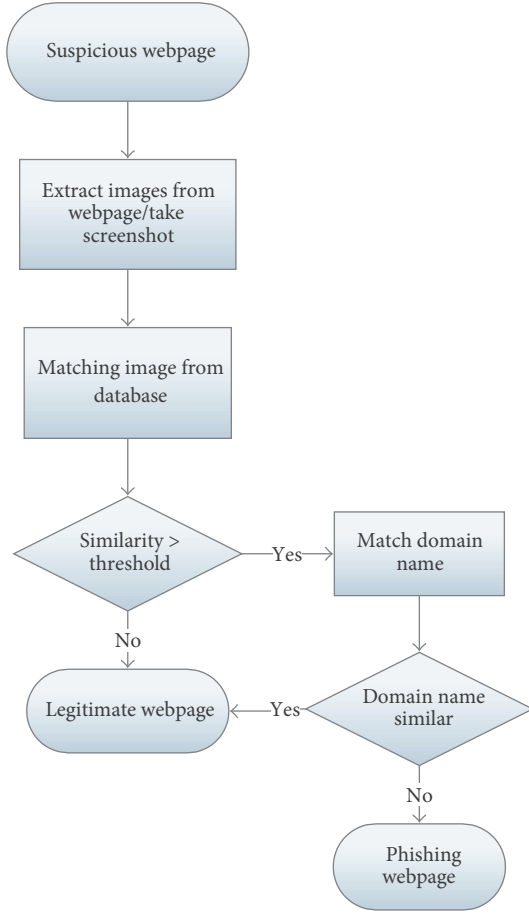
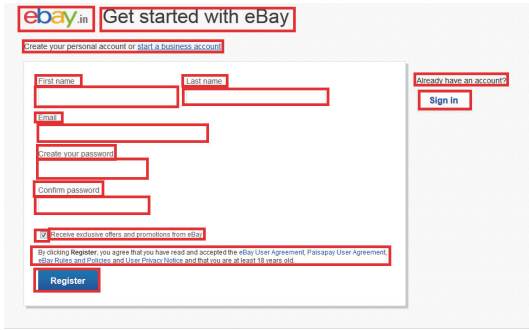FIGURE 12: Detecting of phishing attack using pixel based approach.

FIGURE 13: E-bay phishing webpage: rectangles are the layout blocks.

blocks $y_1, y_2, y_3, \ldots, y_m$. Block similarity is calculated for each block pair (x_i, y_j), $i = 1$ to n and $j = 1$ to m as follows:

$$
\text{Block Similarity (BS)} = \text{mean}\left(\frac{w_{x_i} - w_{y_j}}{T_1}, \frac{h_{x_i} - h_{y_j}}{T_2}, \frac{p_{x_i} - p_{y_j}}{T_3}, \frac{q_{x_i} - q_{y_j}}{T_4}\right), \quad (2)
$$

where T_1 and T_2 are width and height threshold of block and w and h are the width and height of the block. T_3 and T_4 are

the location threshold, and p and q are the horizontal and vertical coordinators of the block.

After block matching, total layout similarity is calculated as follows:

$$
\text{Layout Similarity (LS)} = \frac{\sum_{i=1}^{N_M} \text{BS}_i}{N_M} * \frac{2N_M}{N_X + N_Y}, \quad (3)
$$

where N_X and N_Y are total blocks in webpages X and Y and N_M are total match pair between them. If the layout similarity is greater than certain threshold, then the suspicious webpage is classified as a phishing webpage.

4.4.5. Earth Mover's Distance (EMD). Fu et al. [77] make use of Earth Mover's Distance (EMD) to compare the visual similarity between two webpages. Proposed technique converts the webpage into the low-resolution image (100×100 pixels' images) and then makes the unique signature by using colour features and the centroid of image position. Each pixel is comprised by ARGB (alpha, red, green, and blue) scheme. This approach can only detect phishing webpage if it looks similar to the corresponding legitimate webpage at a certain threshold level. If phishing webpage is partially similar to its legitimate one, then the proposed technique fails to detect it. Approach updates the phishing database at regular intervals from Site Watcher Server.

4.4.6. Victim Information Based Scheme. Hara et al. [70] proposed a phishing detection technique which maintains an image database to compare and determine the nature of the website. Image database contains images and the corresponding domains of the legitimate and phishing websites. The architecture of the approach is shown in Figure 14. The following steps are performed in detection of phishing attack:

Step 1. System captures the images (screenshot) from suspicious URL.

Step 2. Compare the given image with the stored images in the database using ImgSeek [78]; it will find the similar images in the database. After image comparison, the system compares the domain name.

Step 3. If the domain name is not present in the database, it means that the input URL is different, and it is displaying similar images. Therefore, the system declares the given URL phishing. If there is no image in the suspicions website whose similarity is greater than the threshold value, then the proposed techniques return the result as unknown and register the image in the database. For searching images in the database see Algorithm 2.

The comparison of various pixel based approaches (discussed in Section 4.4) on different attacks is presented in Table 3.

4.5. Visual Perception Based Approaches Using Gestalt Theory

4.5.1. Gestalt Theory for Visual Perception. The Gestalt Laws of Organization [80] presented the study of how people
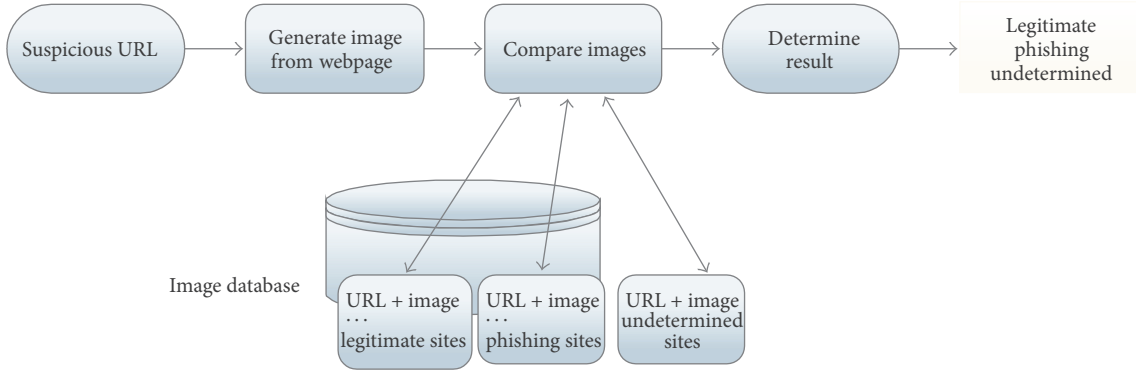
FIGURE 14: Architecture of system [70].

```
(1)  imgSeek(Img_suspicious, Img_legitimate, Img_phish, Img_unknown)
(2)  if (Similarity(Img_suspicious, Img_legitimate) > threshold)
(3)    if (domain(Img_suspicious) = domain(Img_legitimate)) then return("Legitimate")
(4)    else return("Phishing")
(5)    end if
(8)  else
(9)  store_Database({Img_suspicious, domain(Img_suspicious), Unknown})
(10) end if
```

ALGORITHM 2: Algorithm for searching and storing images in database (image seek) [70].

perceive visual components. *Gestalt* is the psychology name which means "unified whole." In this theory, there are six main factors to determine how the visual system automatically groups elements into patterns. These six factors are Proximity, Similarity, Closure, Symmetry, Common Fate (i.e., common motion), and Continuity.

4.5.2. Detecting Visually Similar Webpages: Application to Phishing Detection. Chen et al. proposed [84] an approach that applies the Gestalt theory to identify the visual similarity between two webpages. Author used the concept of supersignals to treat webpages as individual units and compared these particular supersignals using algorithmic complexity theory.

To measure the performance of their approach, they tested group of 12 genuine and 12 phishing webpages in pairs (phishing webpage corresponding to legitimate). After the experiment, they found that all the 12 pairs had been successfully paired together as the most like to one another.

4.6. Hybrid Approaches. Hybrid approaches [79, 81–83] are the combination of two or more types of techniques. Hybrid approaches utilise combination of various features extracted from the webpage like text, images, hyperlinks, and so forth. The accuracy of hybrid approaches is better than the single features based approaches.

4.6.1. Bayesian Approach. Zhang et al. [79] proposed a Bayesian model to determine similarity threshold between suspicious and legitimate webpages. This approach is based on the visual and textual features of a webpage. The Bayesian approach combines the classification results from the textual and visual contents as shown in Figure 15. Textual contents are the words that appear in a webpage, except the articles and stop words (e.g., a, an, the, this, that, etc.). Visual contents are the feature set that includes webpage layout, images, logos, forms, background colour, font colour, and so forth.

The proposed phishing detection system has the following properties:

(i) A naive Bayes rules based text classifier is used to extract text from the webpage.

(ii) Earth Mover's Distance (EMD) based [77] image classifier is used to deal with pixel level contents after transforming the webpage into the image.

(iii) To set the appropriate threshold, a Bayesian approach is used in offline training.

(iv) A Bayesian based fusion algorithm is used to aggregate the results from the image and text classifiers.

There are three major contributions of this approach. First, it presented a text classifier using the naive Bayes rule for phishing detection. Second, it proposed a Bayesian approach to determine the threshold for both the image and text classifiers. Based on this threshold, proposed technique can differentiate between phishing and legitimate webpages. Third, they proposed a new Bayesian approach to combine the classification results from the text and image classifiers.

TABLE 3: Analysis of pixel based techniques on various attacks.

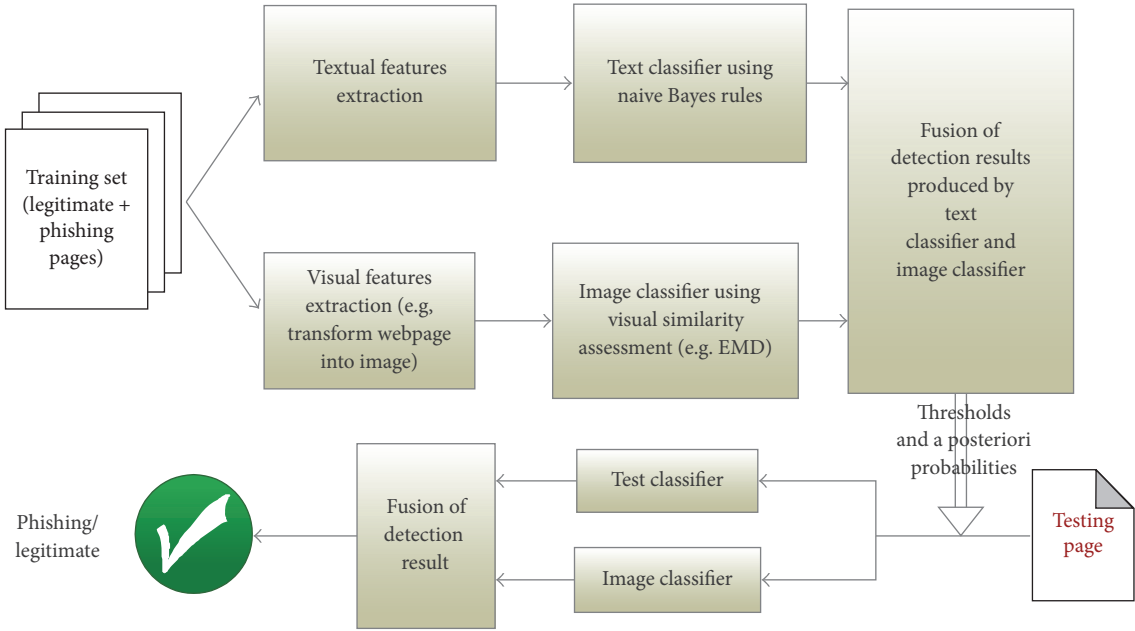| Approach	Zero-hour protection	Embedded object	Language independence	Partially copied webpage	DNS attack
Discriminative keypoint features [72]	×	√	×	×	×
Goldphish [73]	√	√	×	√	×
Dynamic watermarking [74]	×	√	×	×	×
Image layout analysis based approach [75]	×	√	×	×	×
Earth Mover's Distance [77]	×	√	√	×	×
Unknown victim information [70]	×	√	×	×	×

FIGURE 15: Architecture of Bayesian model for phishing detection [79].

4.6.2. Hybrid Features. Medvet et al. [81] proposed an approach which computes a signature using the text, images, and overall visual appearance of the webpage. Text properties extracted from textual content, font size, foreground colour, background colour, font family, and its position in the webpage. Image property includes width, height, src attribute, image position in the webpage, colour histograms [85], and its 2D Haar wavelet transformation. The 2D Haar wavelet transformation provides low-resolution information about the original image.

Signature Comparison. The system starts by comparing matching pairs of elements from each webpage in a website. Matching pairs mean text element only compares with the text and image element only compares with the images. The system then computes text similarity score, image similarity score, and overall visual appearance score. Moreover, total single similarity score $S \in [0, 1]$ is obtained using these three scores (text similarity, image similarity, and overall visual

appearance). The following steps are performed to compare a legitimate webpage with a suspicious webpage:

(1) Take a suspicious webpage "p."

(2) Compute signature $S(p)$ of the suspicious webpage.

(3) Compare the signature of suspicious webpage $S(p)$ with the stored signature of the expected legitimate webpage "p" if the signatures are very much similar, and then invoke an alert.

4.6.3. Automatic Detection of Phishing Target. Liu et al. [82] detect the phishing website by analysing directly and indirectly associated webpages. Directly associated webpages are extracted using hyperlinks present in source code of website. Frequently keywords (using TF-IDF [63] algorithm) are searched for using Google to obtain indirectly associated webpages. After receiving associated webpages, the approach

TABLE 4: Analysis of hybrid approaches on various attacks.

Approach	Zero-hour protection	Embedded object	Language independence	Partially copied webpage	DNS attack
Bayesian model [79]	×	√	×	×	×
Hybrid features [81]	×	√	×	×	×
Using phishing target [82]	√	√	×	√	×
Website logo for phishing detection [83]	√	√	√	√	×

compares given webpage with the associated webpages using the following relations.

(1) Link Relation. It is measured by total number of forwarded link from one webpage to another webpage:

$$L_{xy} = \frac{NL_{xy}}{NL_x}, \tag{4}$$

where NL_{xy} is the number of hyperlinks from webpage "x" to webpage "y" and NL_x is the total hyperlinks present in webpage "x."

(2) Ranking Relation. This relation shows the rank of a webpage in the search engine.

$$R_{xy} = \frac{N_r - (R_s - 1)}{N_r}, \tag{5}$$

where N_r is the total number of search results and R_s is the rank of the domain in the search result.

(3) Text Similarity Relation.

$$TS_{xy} = \cos(i, j) = \frac{i, j}{\|i\| \|j\|}, \tag{6}$$

where TS_{xy} is the text similarity between webpage x and webpage y. i and j are the term vectors obtained from webpage "x" and webpage "y"; $\|i\|$ denotes the length of vector.

(4) Layout Similarity.

$$LS_{xy} = \frac{N_x(\text{blocks}) \cap N_y(\text{blocks})}{N_x(\text{blocks})}, \tag{7}$$

where $N_x(\text{blocks})$ and $N_y(\text{blocks})$ are the total blocks in x and y. $N_x(\text{blocks}) \cap N_y(\text{blocks})$ denotes the common blocks in webpages x and y. By using these four relations, proposed technique can detect the phishing website as well as target of the webpage.

4.6.4. Website Logo for Phishing Detection. Chiew et al. [83] utilise the logo image for phishing detection. The approach is divided into two phases: namely, logo extraction and website identity confirmation. The technique uses the machine learning approach to extract the correct logo image from all images in a website. Furthermore, the correct logo is searched in "Google image" to obtain the corresponding domains.

The returned domains from the search result are used to compare with suspicious website. The proposed technique is the extended work of goldphish [73]. This technique uses the Google image search while goldphish converts logo into text and then converted text used as query on Google. The proposed method has the higher true negative rate as compared to goldphish. The comparison of various hybrid approaches (discussed in Section 4.6) on different attacks is presented in Table 4. Table 5 presents the summary of visual similarity based phishing detection approaches (DOM, visual features, Cascading Style Sheet, pixel based, visual perception, and hybrid approaches) in terms of method use for phishing detection, advantages, and limitations.

5. Performance Evaluation Matrix

Researchers and developers calculate true positive rate, false positive rate, true negative rate, false negative rate, Precision, Recall, accuracy, and $f1$ score of phishing detection system. These are the standard metrics to judge any phishing detection system. Let N_L denote the total number of legitimate websites and N_P denote the total number of phishing websites. Now $N_{L \to L}$ are the legitimate websites classified as legitimate, and $N_{L \to P}$ are the legitimate websites misclassified as phishing. $N_{P \to P}$ are the phishing websites classified as phishing, and $N_{P \to L}$ are the phishing websites misclassified as legitimate. Performance of phishing website detection system can be evaluated in the following manner:

True Positive Rate (TPR). True positive rate is the rate of phishing websites classified as phishing out of total phishing websites.

$$TPR = \frac{N_{P \to P}}{N_P} \times 100. \tag{8}$$

False Positive Rate (FPR). False positive rate is the rate of legitimate websites classified as phishing out of total legitimate sites.

$$FPR = \frac{N_{L \to P}}{N_L} \times 100. \tag{9}$$

False Negative Rate (FNR). False negative rate is the rate of phishing websites classified as legitimate out of total phishing sites.

$$FNR = \frac{N_{P \to L}}{N_P} \times 100. \tag{10}$$

Table 5: Summary of visual similarity based phishing detection techniques.

S. number	Proposed scheme	Description	Advantages	Limitations
1	A layout similarity based approach for detecting phishing pages [48]	HTML DOM based detection	(i) Useful in online banking transaction (ii) High true positive rate (almost 100%)	(i) It fail if attackers create different DOM for similar webpage (ii) It fails if phishing websites only contain images
2	An antiphishing strategy based on visual similarity assessment [66]	Visual features matching, font size, font colour, font family, background and foreground colour, border, and so forth	(i) Detection accuracy is good using visual features	(i) Small dataset used to check performance of the approach (ii) No online detection
3	Mitigate web phishing using site signatures [67]	Text and image based comparison	(i) If only images present (embedded objects) in website, then approach can detect phishing attack	(i) It needs to maintain a large database to store images (ii) It cannot detect zero-hour phishing attack
4	PhishZoo: detecting phishing websites by looking at them [68]	Text, SSL certificate, and images	(i) It gives 96% accuracy (ii) It can detect zero-hour phishing attack	(i) If the logo rotates in phishing website then it cannot detect phishing attack
5	BaitAlarm: detecting phishing sites using similarity in fundamental visual features [71]	CSS based comparison	(i) It can detect embedded object present in a webpage (ii) Good TP rate (more than 99%) (iii) Using large dataset for testing (7764 webpages)	(i) It used previous visited webpages to compare CSS of new page; therefore it cannot detect zero-hour attack
6	Fighting phishing with discriminative keypoint features [72]	Image processing based approach and use of Contrast Context Histogram to compare similarity between pages	(i) If text content is replaced by image or some other embedded objects then this technique can detect it	(i) Passive monitoring of websites (ii) It needs to maintain a large database to store images
7	Goldphish: using images for content-based phishing analysis [73]	Convert logo into text and then use search engine to verify	(i) It can identify well-known popular companies logo (ii) It can detect zero-hour attack	(i) If background of image is dark, then it cannot convert text from images (ii) If sentences are included in the image then it cannot find the relevant site on the search engine
8	Detection and prevention of phishing attack using dynamic watermarking [74]	Dynamic watermarking	(i) It can protect against man in middle attack	(i) High complex, registration required on each unique website for individual user
9	Counteracting phishing page polymorphism: an image layout analysis approach [75]	Compare two images (snapshot of webpage)	(i) It can detect dynamic components like embedded objects and unicode homograph attack (ii) High detection rate, 99.6%	(i) It cannot detect new phishing webpages
10	Detecting phishing web pages with visual similarity assessment based on Earth Mover's Distance (EMD) [77]	Earth Mover's Distance technique is used to compare webpages	(i) It can dynamically adjust threshold by supervised learning (ii) Good precision rate, 99.87%	(i) System fails to detect phishing attack if suspicious site partial copies from legitimate site
11	Visual similarity based phishing detection without victim site information [70]	Image processing based	(i) It does not require the dataset of legitimate websites	(i) When database is empty then consider the new site as a legitimate site (ii) High false positive rate 17.5%
12	Textual and visual content-based antiphishing: a Bayesian approach [79]	Hybrid model, text and image based	(i) The threshold adjusted by the probabilistic model derived from the Bayesian theory	(i) It cannot detect zero-hour attack
13	Visual similarity based phishing detection [81]	Hybrid approach, using image, text, and style similarity	(i) It can detect embedded objects in webpage	(i) It is time-consuming and takes a lot of time to compare text and images (ii) Signature is compared with expected legitimate page; therefore it is difficult to find expected target
14	Detecting visually similar webpages: application to phishing detection [84]	Gestalt theory based on visual perception	(i) It can detect embedded objects (ii) Very low false positive rate, 0.8%	(i) To detect a phishing webpage corresponding legitimate page must be present in the database
15	Automatic detection of phishing target from phishing webpage [82]	Hybrid features, using hyperlinks and keywords from webpage	(i) It can detect zero-hour phishing attack	(i) Accuracy of system depends on the TF-IDF algorithm and search engine
16	Utilisation of website logo for phishing detection [83]	Using machine learning to extract logo, utilised Google image search	(i) It can detect zero-hour phishing attack	(i) High false negative rate, 13%

True Negative Rate (TNR). True negative rate is the rate of legitimate websites classified as legitimate out of total legitimate sites.

$$\text{TNR} = \frac{N_{L \to L}}{N_L}. \tag{11}$$

Accuracy (A). It measures the rate of phishing and legitimate websites which are identified correctly with respect to all the websites.

$$\text{Accuracy} = \frac{N_{L \to L} + N_{P \to P}}{N_L + N_P} \times 100. \tag{12}$$

Precision (P). It measures the rate of phishing websites which are correctly identified with respect to websites detected as phishing:

$$\text{Precision} = \frac{N_{P \to P}}{N_{P \to P} + N_{L \to P}} \times 100. \tag{13}$$

Recall (R). It measures the rate of phishing websites which are correctly identified with respect to correctly classified phishing and legitimate websites.

$$\text{Recall} = \frac{N_{P \to P}}{N_{P \to P} + N_{L \to L}} \times 100. \tag{14}$$

f1 Score. It is the harmonic mean of Precision and Recall.

$$f1 \ \text{score} = \frac{2 \times P \times R}{P + R}. \tag{15}$$

6. Open Issues and Challenges

Various types of antiphishing techniques based on visual similarity approach have been given in the literature. However, still there is no single technique that can detect all types of phishing attacks (i.e., zero-hour phishing attack, embedded objects, DNS poisoning, etc.). Day by day phishing attack is increasing continuously and becomes the most popular e-crime. Consistently, when researchers design a new technique to control phishing attack, attackers change their way to perform attack or exploit the vulnerability in the solution. Hence, there is the tight race between attackers and antiphishing developers. There are various issues which have to take care while designing a new antiphishing technique. The first problem is the zero-hour phishing attack. Most of the antiphishing techniques [48, 66, 67] compare the suspicious website from the pool of legitimate sites using feature set including URL, keyword, and visual appearances. These techniques required a large dataset and still fail to detect zero-hour phishing attack. If attacker designs a new webpage and its target (corresponding legitimate page) is not available in the dataset, then technique fails to detect new fake webpages (zero- hour attack). Liu et al. [82] presented a technique which can detect zero-hour phishing attack; however this technique depends on the TF-IDF algorithm and hyperlinks. Therefore, detection of zero-hour phishing

attack with high accuracy is still an open challenge. The second issue is the language independence. Various text languages are worldwide used in the websites, and the e-commerce and banking websites also have different text languages in various countries for example, Amazon, eBay, and Citibank. The layout of e-commerce and banking sites is almost similar in different languages. Heuristics based phishing detection techniques [54, 69, 86, 87] use the keywords, and they are language dependent. As we discussed, some of the visual feature based techniques [48, 71] can detect this attack because they utilise the webpage features like the logo of the company, CSS Structure, DOM tree, and so forth. Such techniques only detect the attack if the layout of phishing website is similar to the real one. However, these techniques are unable to detect a new phishing attack (zero-hour) because they compare the current website with the stored database. The third issue is the embedded objects present in the webpage as attackers use images, JavaScript, and so forth, to bypass the antiphishing system. As we discussed, image processing based techniques [72–75] can detect the embedded objects present in suspicious webpage because these techniques take the snapshot of the webpage and compare it with the corresponding legitimate webpage. But identifying the correct corresponding legitimate webpage is the major problem in image processing based solutions. Image processing based approaches also consumed a lot of time to compare a suspicious website with the pool of websites. Therefore detection of phishing site which uses embedded objects is still an open challenge. The fourth issue is determining an appropriate threshold to take appropriate decision. The threshold is the matching score between two websites. As we discussed, attacker constructs a phishing website which looks similar to legitimate one. If the phishing website is partially copied (less than 50%) from the legitimate website, then none of the visual similarity based approach can detect it. Therefore, adjusting the appropriate threshold to detect a maximum number of phishing websites is a challenging task. If antiphishing system increases the threshold then the false negative rate increases and if it decreases the threshold then false positive rate increases [48] as shown in Figure 16. A good antiphishing system requires that both false negative and false positive rate should be as minimal as possible.

7. Conclusion

Phishing is an appalling threat in the web security domain. In this attack, the user inputs his/her personal information to a fake website which looks like a legitimate one. We have presented a survey on phishing detection approaches based on visual similarity. This survey provides a better understanding of phishing website, various solution, and future scope in phishing detection. Many approaches are discussed in this paper for phishing detection; however most of the approaches still have limitations like accuracy, the countermeasure against new phishing websites, failing to detect embedded objects, and so forth. These approaches use various features of a webpage to detect phishing attacks, such as text similarity, font colour, font size, and images present in
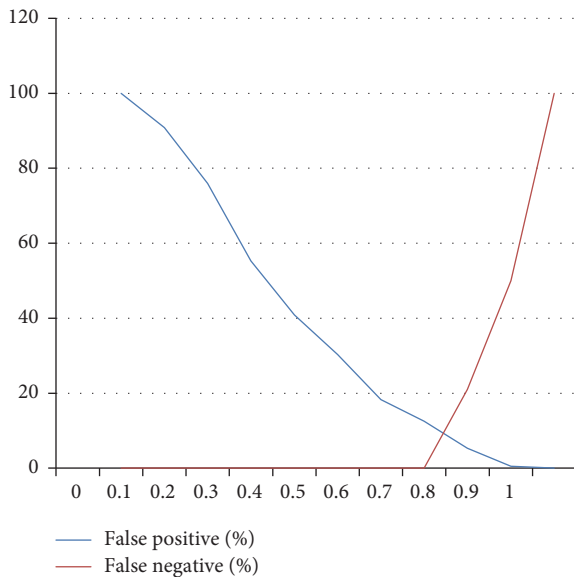
FIGURE 16: False positive and false negative rate on different threshold [48].

the webpage. Text based similarity approaches are relatively fast, but they are unable to detect phishing attack if the text is replaced with some image. Image processing based approaches have high accuracy rate while they are complex in nature and are time-consuming. Furthermore, most of the work is done offline. These involve data collection and profile-creation phases to be completed first. A comparative table is prepared for easy glancing at the advantages and drawbacks of the available approaches. No single technique is enough for adopting it for phishing detection purposes. Detection of phishing websites with high accuracy is still an open challenge for further research and development.

Competing Interests

The authors declare that they have no competing interests.

References

[1] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013.

[2] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 324–335, 2013.

[3] A. K. Jain and B. B. Gupta, "Comparative analysis of features based machine learning approaches for phishing detection," in *Proceedings of the 10th INDIA-COM*, New Delhi, India, 2016.

[4] G. Weaver, A. Furr, and R. Norton, *Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-Day Phishing Attacks on Universities*, 2016.

[5] Kaspersky Lab, "Spam in January 2012 love, politics and sport," 2013, http://www.kaspersky.com/about/news/spam/2012/Spam_in_January_2012_Love_Politics_and_Sport.

[6] APWG Q1-Q3 Report, 2015, http://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf.

[7] B. Parmar, "Protecting against spear-phishing," *Computer Fraud & Security*, vol. 2012, no. 1, pp. 8–11, 2012.

[8] W. Jingguo, T. Herath, C. Rui, A. Vishwanath, and H. R. Rao, "Phishing susceptibility: an investigation into the processing of a targeted spear phishing e-mail," *IEEE Transactions on Professional Communication*, vol. 55, no. 4, pp. 345–362, 2012.

[9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[10] C. H. Hsu, P. Wang, and S. Pu, "Identify fixed-path phishing attack by STC," in *Proceedings of the 8th Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS '11)*, pp. 172–175, ACM, Perth, Australia, September 2011.

[11] N. A. G. Arachchilage and M. Cole, "Designing a mobile game for home computer users to protect against phishing attacks," https://arxiv.org/abs/1602.03929.

[12] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '05)*, pp. 77–88, July 2005.

[13] S. Sheng, B. Magnien, P. Kumaraguru et al., "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*, Pittsburgh, Pa, USA, July 2007.

[14] K.-P. Yee and K. Sitaker, "Passpet: convenient password management and phishing protection," in *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS '06)*, pp. 32–43, ACM, Pittsburgh, Pa, USA, July 2006.

[15] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth, "An evaluation of extended validation and picture-in-picture phishing attacks," in *Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security (FC '07/USEC '07)*, pp. 281–293, Springer, Scarborough, UK, February 2007.

[16] M. Jakobsson, "Modeling and preventing phishing attacks," in *Proceedings of the 9th International Conference on Financial Cryptography and Data Security*, Roseau, Dominica, February-March 2005.

[17] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," in *Proceedings of the Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit*, pp. 1–13, Pittsburgh, Pa, USA, October 2007.

[18] L. James, *Phishing Exposed*, Syngress Publishing, 2005.

[19] L. H. Lee, K. Lee, Y. Juan, H. Chen, and Y. Tseng, "Users' behavioral prediction for phishing detection," in *Proceedings of the the 23rd International World Wide Web Conference*, pp. 337–338, Seoul, Republic of Korea, April 2014.

[20] X. Chen, I. Bose, A. C. M. Leung, and C. Guo, "Assessing the severity of phishing attacks: a hybrid data mining approach," *Decision Support Systems*, vol. 50, no. 4, pp. 662–672, 2011.

[21] M. Moghimi and A. Y. Varjani, "New rule-based phishing detection method," *Expert Systems with Applications*, vol. 53, pp. 231–242, 2016.

[22] G. Ramesh, I. Krishnamurthi, and K. S. S. Kumar, "An efficacious method for detecting phishing webpages through target domain identification," *Decision Support Systems*, vol. 61, no. 1, pp. 12–22, 2014.

[23] P. Beatty, I. Reay, S. Dick, and J. Miller, "Consumer trust in e-commerce web sites: a meta-study," *ACM Computing Surveys*, vol. 43, no. 3, article 14, 46 pages, 2011.

[24] J. M. Pavía, E. J. Veres-Ferrer, and G. Foix-Escura, "Credit card incidents and control systems," *International Journal of Information Management*, vol. 32, no. 6, pp. 501–503, 2012.

[25] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. Christopher Westland, "Data mining for credit card fraud: a comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.

[26] M. T. Banday and J. A. Qadri, "Phishing—a growing threat to E-commerce," *The Business Review*, vol. 12, no. 2, pp. 76–83, 2007.

[27] J. Efrim Boritz and W. G. No, "E-commerce and privacy: Exploring what we know and opportunities for future discovery," *Journal of Information Systems*, vol. 25, no. 2, pp. 11–45, 2011.

[28] Y. Zhang, X. Deng, D. Wei, and Y. Deng, "Assessment of E-Commerce security using AHP and evidential reasoning," *Expert Systems with Applications*, vol. 39, no. 3, pp. 3611–3623, 2012.

[29] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7913–7921, 2010.

[30] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Associative classification techniques for predicting e-banking phishing websites," in *Proceedings of the International Conference on Multimedia Computing and Information Technology (MCIT '10)*, pp. 9–12, IEEE, Sharjah, UAE, March 2010.

[31] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Experimental case studies for investigating E-banking phishing techniques and attack strategies," *Cognitive Computation*, vol. 2, no. 3, pp. 242–253, 2010.

[32] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the internet: attacks, costs and responses," *Information Systems*, vol. 36, no. 3, pp. 675–705, 2011.

[33] G. Megaw and S. V. Flowerday, "Phishing within e-commerce: a trust and confidence game," in *Proceedings of the Information Security for South Africa (ISSA '10)*, pp. 1–8, IEEE, Johannesburg, South Africa, August 2010.

[34] A. Litan, *Phishing Attack Victims Likely Targets for Identity Theft*, Gartner Group, 2004.

[35] A. Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paaß, and S. Strobel, "New filtering approaches for phishing email," *Journal of Computer Security*, vol. 18, no. 1, pp. 7–35, 2010.

[36] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.

[37] M. Jakobsson and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, Wiley-Interscience, 2006.

[38] Internet world stats—usage and population statistics, 2014, http://www.internetworldstats.com/stats.htm.

[39] RSA Anti-Fraud Command Center, RSA monthly online fraud report, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf.

[40] Anti-Phishing Working Group (APWG), Phishing activity trends report first quarter 2014, http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf.

[41] APWG report, http://apwg.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf.

[42] RSA Current State of Cybercrime, https://www.rsa.com/en-us/perspectives/industry/online-fraud.

[43] C. Kruegel, E. Kirda, D. Mutz, W. Robertson, and G. Vigna, "Automating mimicry attacks using static binary analysis," in *Proceedings of the USENIX Security Symposium*, pp. 161–176, Baltimore, Md, USA, 2005.

[44] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2070–2090, 2013.

[45] A. Tewari, A. K. Jain, and B. B. Gupta, "Recent survey of various defense mechanisms against phishing attacks," *Journal of Information Privacy and Security*, vol. 12, no. 1, pp. 3–13, 2016.

[46] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications*, 2016.

[47] R. Dhamija, J. D. Tygar, and M. A. Hearst, "Why phishing works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*, pp. 581–590, ACM Press, 2006.

[48] A. P. E. Rosiello, E. Kirda, C. Kruegel, and F. Ferrandi, "A layout-similarity-based approach for detecting phishing pages," in *Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm '07)*, pp. 454–463, September 2007.

[49] A. K. Jain and B. B. Gupta, "PHISH-SAFE URL: features based phishing detection system using machine learning," in *Proceedings of the Golden Jubilee Year of the Computer Society of India (CSI '15)*, New Delhi, India, December 2015.

[50] V. Ramanathan and H. Wechsler, "PhishGILLNET-phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training," *Eurasip Journal on Information Security*, vol. 2012, article 1, 2012.

[51] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An empirical analysis of phishing black-lists," in *Proceedings of the 6th Conference on E-Mail and Anti-Spam (CEAS '09)*, 2009.

[52] P. Prakash, M. Kumar, R. Rao, and M. Gupta, "Phishnet predictive black-listing to detect phishing attacks," in *Proceedings of the 29th Conference on Information Communications*, pp. 346–350, San Diego, Calif, USA, 2010.

[53] A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using auto-updated white-list," *EURASIP Journal on Information Security*, vol. 2016, article 9, 11 pages, 2016.

[54] G. A. Montazer and S. Yarmohammadi, "Detection of phishing attacks in Iranian e-banking using a fuzzy-rough hybrid system," *Applied Soft Computing*, vol. 35, pp. 482–492, 2015.

[55] B. Gu, V. S. Sheng, Z. Wang, D. Ho, S. Osman, and S. Li, "Incremental learning for ν-Support Vector Regression," *Neural Networks*, vol. 67, pp. 140–150, 2015.

[56] B. B. Gupta, D. P. Agrawal, and S. Yamaguchi, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global, Hershey, Pa, USA, 2016.

[57] B. Gu, V. S. Sheng, K. Y. Tay, W. Romano, and S. Li, "Incremental support vector learning for ordinal regression," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 7, pp. 1403–1416, 2015.

[58] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," in *Proceedings of the 2nd Annual eCrime Researchers Summit (eCrime '07)*, pp. 60–69, ACM, Pittsburgh, Pa, USA, 2007.

[59] A. ALmomani, B. B. Gupta, T.-C. Wan, A. Altaher, and S. Manickam, "Phishing dynamic evolving neural fuzzy framework for online detection 'zero-day' phishing E-mail," *Indian Journal of Science and Technology*, vol. 6, no. 1, pp. 3960–3964, 2013.

[60] R. M. Basnet, S. Mukkamala, and A. H. Sung, "Detection of phishing attacks: a machine learning approach," *Studies in Fuzziness and Soft Computing*, vol. 226, pp. 373–383, 2008.

[61] W. Han, Y. Cao, E. Bertino, and J. Yong, "Using automated individual white-list to protect web digital identities," *Expert Systems with Applications*, vol. 39, no. 15, pp. 11861–11869, 2012.

[62] Y. Cao, W. Han, and Y. Le, "Anti-phishing based on automated individual white-list," in *Proceedings of the 4th ACM Workshop on Digital Identity Management (DIM '08)*, pp. 51–60, ACM, 2008.

[63] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: a content-based approach to detecting phishing web sites," in *Proceedings of the 16th International World Wide Web Conference (WWW '07)*, pp. 639–648, Banff, Canda, May 2007.

[64] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "CANTINA+: a feature-rich machine learning framework for detecting phishing web sites," *ACM Transactions on Information and System Security*, vol. 14, no. 2, article 21, 2011.

[65] F. Harary, *Graph Theory*, Addison-Wesley, 1969.

[66] W. Liu, X. Deng, G. Huang, and A. Y. Fu, "An antiphishing strategy based on visual similarity assessment," *IEEE Internet Computing*, vol. 10, no. 2, pp. 58–65, 2006.

[67] C.-Y. Huang, S.-P. Ma, W.-L. Yeh, C.-Y. Lin, and C.-T. Liu, "Mitigate web phishing using site signatures," in *Proceedings of the IEEE Region 10 Conference TENCON*, pp. 803–808, November 2010.

[68] S. Afroz and R. Greenstadt, "PhishZoo: detecting phishing websites by looking at them," in *Proceedings of the 5th Annual IEEE International Conference on Semantic Computing (ICSC '11)*, pp. 368–375, Palo Alto, Calif, USA, September 2011.

[69] A. Mishra and B. B. Gupta, "Hybrid solution to detect and filter zero-day phishing attacks," in *Proceedings of the Emerging Research in Computing, Information, Communication and Applications (ERCICA '14)*, Bangalore, India, August 2014.

[70] M. Hara, A. Yamada, and Y. Miyake, "Visual similarity-based phishing detection without victim site information," in *Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS '09)*, pp. 30–36, IEEE, Nashville, Tenn, USA, April 2009.

[71] J. Mao, P. Li, K. Li, T. Wei, and Z. Liang, "BaitAlarm: detecting phishing sites using similarity in fundamental visual features," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13)*, pp. 790–795, Xi'an, China, September 2013.

[72] K.-T. Chen, J.-Y. Chen, C.-R. Huang, and C.-S. Chen, "Fighting phishing with discriminative keypoint features," *IEEE Internet Computing*, vol. 13, no. 3, pp. 56–63, 2009.

[73] M. Dunlop, S. Groat, and D. Shelly, "GoldPhish: using images for content-based phishing analysis," in *Proceedings of the 5th International Conference on Internet Monitoring and Protection (ICIMP '10)*, pp. 123–128, Barcelona, Spain, May 2010.

[74] A. P. Singh, V. Kumar, S. Sengar, and M. Wairiya, "Detection and prevention of phishing attack using dynamic watermarking," in *Information Technology and Mobile Communication*, Communications in Computer and Information Science, pp. 132–137, Springer, 2011.

[75] I.-F. Lam, W.-C. Xiao, S.-C. Wang, and K.-T. Chen, "Counteracting phishing page polymorphism: an image layout analysis approach," in *Proceedings of the 3rd International Conference and Workshops on Advances in Information Security and Assurance*, pp. 270–279, Seoul, Republic of Korea, 2009.

[76] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Transactions on Systems Man and Cybernetics*, vol. 9, no. 1, pp. 62–66, 1979.

[77] A. Y. Fu, W. Liu, and X. Deng, "Detecting phishing web pages with visual similarity assessment based on Earth Mover's Distance (EMD)," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 301–311, 2006.

[78] C. Jacobs, A. Finkelstein, and D. Salesin, "Fast multi resolution image querying," in *Proceedings of the 22nd Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH '95)*, pp. 277–286, Los Angeles, Calif, USA, August 1995.

[79] H. Zhang, G. Liu, T. W. S. Chow, and W. Liu, "Textual and visual content-based anti-phishing: a Bayesian approach," *IEEE Transactions on Neural Networks*, vol. 22, no. 10, pp. 1532–1546, 2011.

[80] M. Ertheimer, *Gestalt Theory*, Hayes Barton Press, New York, NY, USA, 1944.

[81] E. Medvet, E. Kirda, and C. Kruegel, "Visual-similarity-based phishing detection," in *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureComm '08)*, 245, 234 pages, İstanbul, Turkey, September 2008.

[82] G. Liu, B. Qiu, and L. Wenyin, "Automatic detection of phishing target from phishing webpage," in *Proceedings of the 20th International Conference on Pattern Recognition (ICPR '10)*, pp. 4153–4156, Istanbul, Turkey, 2010.

[83] K. L. Chiew, E. H. Chang, S. N. Sze, and W. K. Tiong, "Utilisation of website logo for phishing detection," *Computers & Security*, vol. 54, pp. 16–26, 2015.

[84] T.-C. Chen, S. Dick, and J. Miller, "Detecting visually similar web pages: application to phishing detection," *ACM Transactions on Internet Technology*, vol. 10, no. 2, article 5, 38 pages, 2010.

[85] C.-R. Huang, C.-S. Chen, and P.-C. Chung, "Contrast context histogram—an efficient discriminating local descriptor for object recognition and image matching," *Pattern Recognition*, vol. 41, no. 10, pp. 3071–3077, 2008.

[86] P. A. Barraclough, M. A. Hossain, M. A. Tahir, G. Sexton, and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions," *Expert Systems with Applications*, vol. 40, no. 11, pp. 4697–4706, 2013.

[87] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "The design of phishing studies: challenges for researchers," *Computers & Security*, vol. 52, pp. 194–206, 2015.