A report on

VISUAL CRYPTOGRAPHY AND ITS APPLICATIONS

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI

ज्ञानं परमं बलम्

Apoorv Singh	2018A3PS0640G
Archish De	2018A7PS0149G
Arjun Agarwal	2017B3S70285G
Harsh Srivastava	2017A4PS0924G

Table Of Contents

- Abstract……………………………………………………………………………3
- Introduction…………………………………………………………………..3
- Motivation……………………………………………………………………...3
- Visual Cryptography Schemes for Black and White images……………………...4
    - (K, N) secret sharing technique…………………………………………...4
        - Shamir's secret sharing technique………………………………...4.
        - (2, N) secret sharing technique……………………………………4
    - Advantages and disadvantages……………………………………………7
- Image encryption using keys……………………………………………………..9
- Applications of Visual Cryptography…………………………………………....16
    - Biometric Authentication…………………………………………….....16
    - Digital Image Copyright Protection……………………………….…18
- Conclusion………………………………………………………………….21
- References……………………………………………………………….....23

Abstract

This study is about a pedagogically unconventional cryptographic technique called “Visual Cryptography” and its implementation and applications in the real world problems. We discuss different schemes like (K, N) secret sharing technique, image encryption using keys. The following schemes were also successfully implemented. Their advantages and disadvantages were also compared with the standard encryption schemes like AES, RSA. Apart from implementation, some applications like their use in increasing security of Biometric Authentication and in Digital Image copyright protection were also studied and implemented.

Introduction

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image. It was developed by Moni Naor and Adi Shamir, in 1994. The concept was to create an image sharing scheme, in which an image was broken into N different shares and a person with all the N different shares can only decrypt to the original image. All of these N shares need to be superimposed on each other, to recover the original image. Later on more general schemes were developed in which only K out of N shares were required in order to successfully decrypt to the original image.

Visual cryptography has a vast number of applications including biometric authentication and secure data storage. It also provides strong support to non-visual cryptography (i.e. Symmetric key algorithms etc.) by increasing the security multifold. It has also found it’s usages in data hiding.

Motivation

Nowadays, in the Internet, besides text, multimedia information is also quite prevalent. Therefore the security of these secret and confidential images is a valid concern, where VCS can be helpful. The important idea behind Visual Cryptography is to encrypt information in the form of images in a secure and flawless way. The information is divided in N shares before it is sent, so that it cannot be illegally read or modified in the middle of transmission.

Visual Cryptography Schemes on Black and White images

Due to the vast number of representations of an image (Greyscale, RGB, RGBA, halftone etc.) different methods need to be employed for each category. However the core concept remains the same:

- **(K, N) secret sharing technique**
    - **Shamir's secret sharing technique**

      The (K, N) secret sharing technique is based on an idea introduced by Adi Shamir. The crux of this technique is that a secret is divided into n unique "shares" and distributed among n participants, giving each participant his/her own share. To reconstruct the original secret, a minimum of k shares (called the threshold) are required to be brought together. However, combining any combination of less than K shares should provide no clue towards the original secret.

      A higher value of K is desirable (but usually more difficult to achieve) since a greater number of shares have to be brought together in order to reconstruct the secret. When K = N, all the shares are required to reconstruct the original secret.

    - **(2, N) secret sharing technique**

      This is a special case of the (K, N) secret sharing technique where K = 2. This means that if any two shares are combined, the original secret is reconstructed. Let us see how it works:

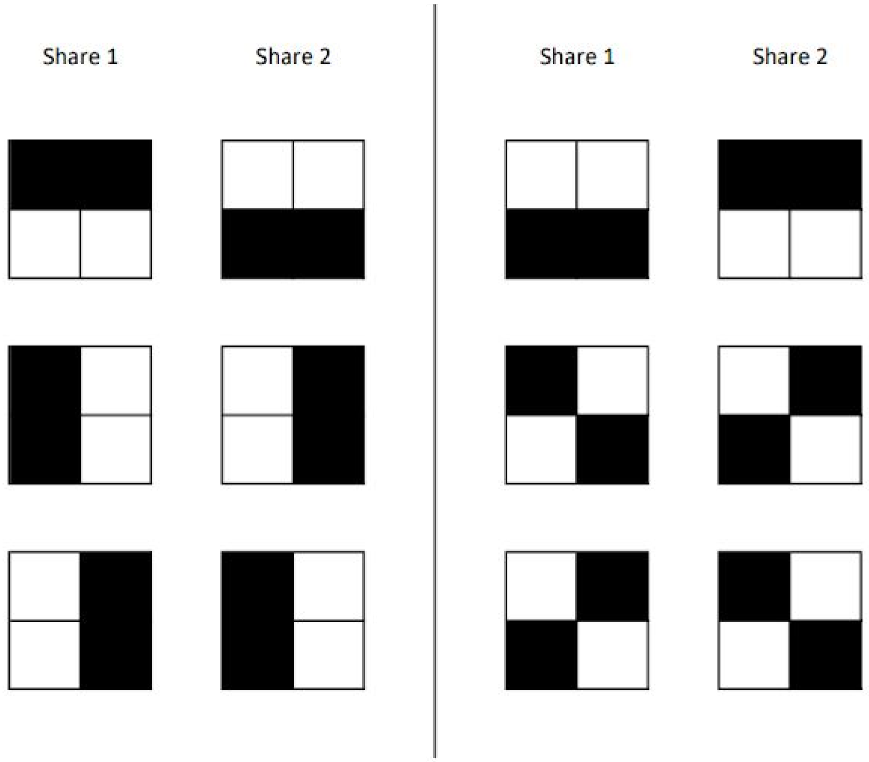
      Splitting the secret:

      We iterate over all the pixels of the black and white image. Each pixel is represented by 4 subpixels in each of the shares. The original pixel may either be black or white. Let us look at what we do in each case:

      Black pixel:

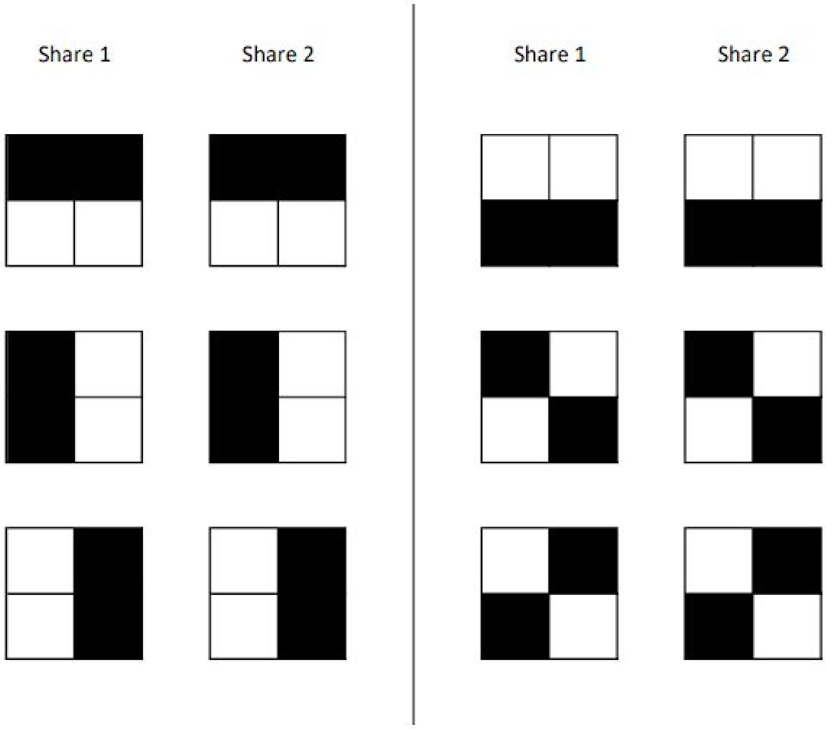
Here, we colour two of the subpixels black in one share and the other two subpixels in the other share. The decision of which two subpixels should be coloured in the first share is chosen randomly (among 4C2 = 6 ways) and hence the subpixels of the other share are automatically decided.

The six different possibilities are:



White pixel:

Here also we select two subpixels at random from the first share and colour them black. However, instead of colouring the remaining two black in the second share, we colour the same two pixels black. Therefore, the possibilities are:



Combining the shares:

To combine the two shares, just overlap the shares on top of each other (where a black pixel is assumed to be coloured and a white pixel is assumed to be transparent). This is equivalent to the logical OR operator on each subpixel i.e. a pixel will be coloured if (the corresponding pixel in share 1 is coloured) OR (the corresponding pixel in share 2 is coloured) OR … OR (the corresponding pixel in share t is coloured)

If the pixel was black in the original secret, the four subpixels will all be coloured black when the shares are combined because of the way it was split into shares. However, when a pixel which was white in the original secret will appear to have half of the subpixels coloured black and the remaining to be coloured white.

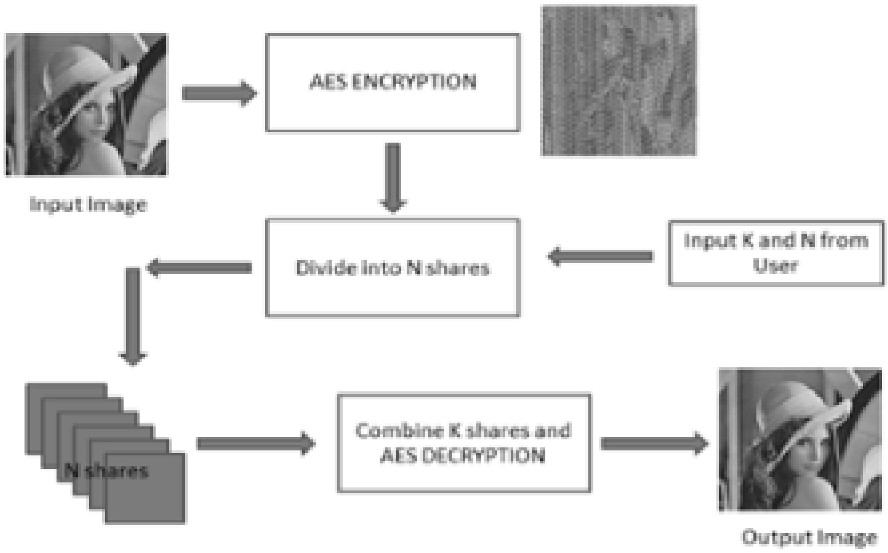
However, analyzing a single share will give us no information at all since each combination of subpixels will have two of the subpixels black and the remaining two white and so the colour of the original pixel cannot be deduced.

Note: It is not necessary to use a 2 X 2 grid of subpixels for each pixel of the original secret. We can use any combination i.e. an M X N grid. However, if M ≠ N, the aspect ratio of the image changes which is why it is always preferable to have M = N. The subpixels chosen to be coloured has to be adjusted accordingly.

There have been many different methods proposed on how to go about (K, N) secret sharing, each having their own merits and demerits. Let us discuss these and how this fares against non-visual cryptography:

- The advantages are:
  - ○ The combination of shares can only be decrypted by the eye. No information can be obtained by looking at the pixels individually as their colour is decided independently while splitting the secret.
  - ○ Can be combined with non-visual cryptography effortlessly even though they operate in a very different manner

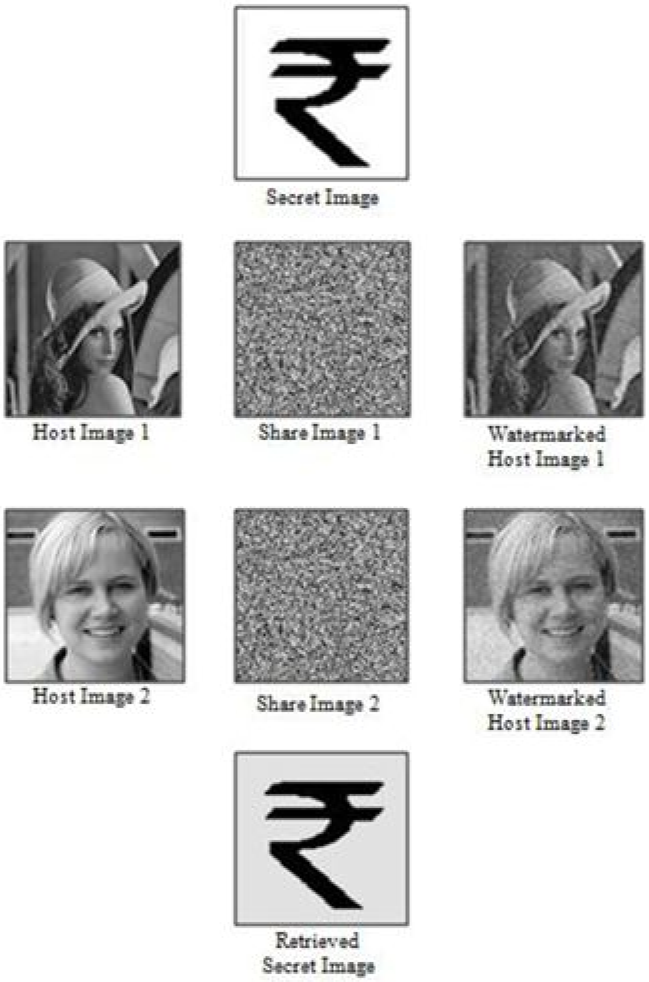
    Eg. of one such combination (using AES and (K, N) secret sharing)



  - ○ When combined with non-visual cryptography, the security of the encryption increases exponentially which is highly desirable.

  - (K, N) secret sharing in visual cryptography has very strong applications in visual steganography.

    Eg.



  - Interception of packets on the internet, letters in the mail etc. are punishable by law in almost all countries, not to mention difficult. Since (K, N) secret sharing requires multiple messages to be sent over from one location to another (may be through various channels), intercepting the messages is that much harder (and illegal) which will make the attacker "Oscar" much more skeptical.
- Disadvantages of (K, N) secret sharing technique:
  - The shares formed and the final image after combining the shares have a much

higher pixel count (4 times the original secret in the (2, N) case) since each pixel of the original secret is blown up into multiple subpixels. This leads to an increase in size of the file which has to be transmitted over the channel(s).

However, more recent methodologies of implementing (K, N) secret sharing have overcome this obstacle by using boolean vectors, smart distribution of coloured subpixels, replacing the OR function with the logical XOR function, and a simple usage of the pigeonhole principle.

- Splitting up and combining bigger images is very costly as each pixel has to be read separately. However, since the computations are independent between pixels, we can employ the use of parallelism (such as software/hardware threading) to make the process faster.
- Since decryption can be done only by the eye, this technique has to be used conservatively unless trustworthy additional manpower can be employed.
- The final image may be distorted or may have a different aspect ratio from the original image depending on the implementation of the technique.
- Does not stop Oscar from deciphering the secret if he is able to get his hands on the required K shares. Therefore, it is advised to combine it with non-visual cryptography for optimum usage.

Implementation of (K, N) secret sharing technique

In the project, a black and white image was taken and split into two shares. It was clearly seen that the two shares provided no indication whatsoever as to what the original image was. However on superimposing the two images, the original black and white image was retrieved and the secret message became visible.

Image Encryption using keys

Image encryption can be defined as the process of encoding a secret image with the help of some encryption algorithm in such a way that the encrypted image is unrecognizable to unauthorized users.

The problem of security in transmission of confidential visual information exists in a variety of applications. Most conventional ciphers such as DES, AES and LFSR are not suitable for image encryption in real time because of their slow speed due to large data volume, and strong correlation between pixels.

Chaos theory in cryptography:

A chaotic system is a deterministic system that exhibits seemingly random behaviour as a result of its sensitive dependence on its initial conditions. A chaotic system resembles noise.

The basic principle of image encryption using chaos is based on the ability of some dynamic systems to produce sequences of numbers that are random in nature. Messages are encrypted using these sequences.

The confusion stage is the pixel permutation where the positions of the pixels are scrambled over the entire image without disturbing the values of the pixels. With this the image becomes unrecognizable.

To enhance the security, the second stage of the encryption process aims at changing the value of each pixel in the entire image. The process of diffusion is carried out through a chaotic map which is mainly dependent on the initial conditions and control parameters.

In the diffusion stage, the pixel values are modified sequentially by the sequence generated from the chaotic systems. The whole confusion-diffusion round repeats for a number of times to achieve security of satisfactory level. The randomness property which is inherent in chaotic maps makes it more suitable for image encryption

Logistic Map:

The logistic map is a polynomial mapping of degree 2. The equation of the map is as follows:

$X(n+1) = mu * X(n) * (1-X(n))$

Where mu and X_0 are the control parameters.

By varying the parameter mu, the following observations are observed:

- When the value of μ lies between 2 and 3, the iterative values first oscillate around some value and then finally stabilize on the same value.
- When the value of μ lies between 3 and 3.45 (approximately), the iterative values oscillate between two values forever, which are dependent on μ
- When the value of μ lies between 3.45 and 3.56 (approximately), the iterative values oscillate between four values.
- As the value of μ becomes greater than or equal to 3.57, this logistic map is converted into a chaotic map because a slight variation in the initial condition produces dramatically different iterative values over time. This condition is suitable for image encryption.

The cryptosystem:

The cryptosystem which I designed converts a grayscale image into an encrypted version. I use row wise and column wise circular left and right shifts to permute the pixels in the confusion stage. I then use XOR operations on each individual pixel to change the grayscale value of the pixel. Finally, I use a chaotic logistic map and the XOR operation for the final diffusion of the image. This procedure is repeated 10 times. The experimental result and security analysis show that this algorithm can resist exhaustive attacks, statistical attacks, and differential attacks.

The Encryption Algorithm:

Let I represent the grayscale image of size M x N.

Step 1: Generate randomly two vectors K_R and K_C of length M and N, respectively. The vectors take random values between 0 and 255 (for an 8 bit grayscale image).

Step 2: Decide the number of iterations ITER = 10

Step 3: Generate a vector X_0 containing ITER values. Each value will be randomly generated in the following manner:

Step 3.1: Generate 16 8-bit numbers.

Step 3.2: Take the sum of all the number and divide by prime number 4091 to get an irrational number

Step 3.3: Take the number modulo 1 to get rid of the integral part.

Step 4: For each row i of image I:

Step 4.1: Compute the sum of all elements in the row denoted by a_i

Step 4.2: Compute a_i modulo 2 denoted by Ma_i

Step 4.3: If $Ma_i = 0$, right circular shift by $K_r(i)$ positions, else left circular shift.

Step 5: For each column j of image I:

Step 5.1: Compute the sum of all elements in the row denoted by b_i

Step 5.2: Compute b_i modulo 2 denoted by Mb_i

Step 5.3: If $Ma_i = 0$, up circular shift by $K_r(i)$ positions, else down circular shift.

Step 6: Using vector K_C, the bitwise XOR operator is applied to each row of scrambled image I using the following expressions:

- $I(2i-1,j)=I(2i-1,j) \oplus K_C(j)$,
- $I(2i,j)=I(2i,j) \oplus \mathrm{rot180}(K_C(j))$

Where $\oplus$ and rot180(KC) represent the bitwise XOR operator and the flipping of vector K_C from left to right, respectively.

Step 7: Using vector K_R, the bitwise XOR operator is applied to each column of image I using the following formulas:

- $I(i,2j-1)=I(i,2j-1)\oplus K_R(j)$,
- $I(i,2j)=I(i,2j)\oplus \mathrm{rot180}(K_R(j))$

Step 8: Calculate M x N values of the logistic map using $X_0(i)$ as the initial value and Mu = 3.9999.

$X_{n+1} = Mu*X_n*(1-X_n)$

Step 9: Xi = int(Xi*10^16)%256, where int(x) represents the integral part of x

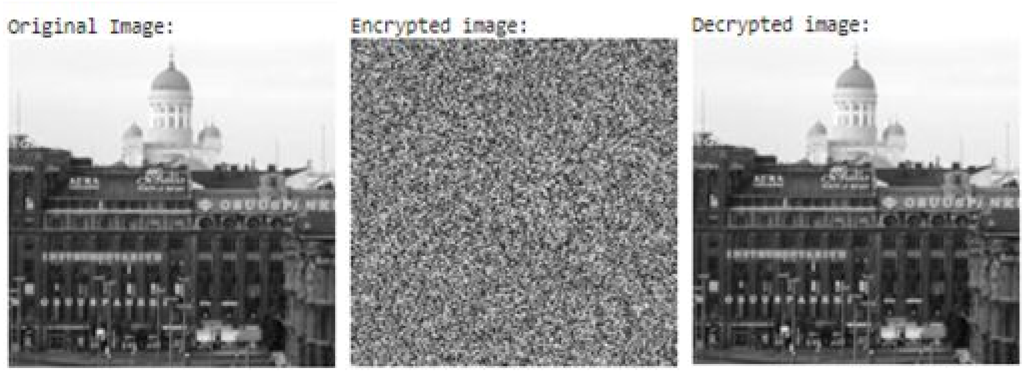
Step 10: For each pixel p of the image I,

- $p_i = p_i \wedge x_i$ if i = 0
- $p_i = (p_i+p_{i-1})\%256 \wedge x_i$, otherwise

Step 11: Repeat step 3 to 11 ITER times.

Note: The decryption algorithm is just the inverse of the encryption algorithm.

Experimental Results:



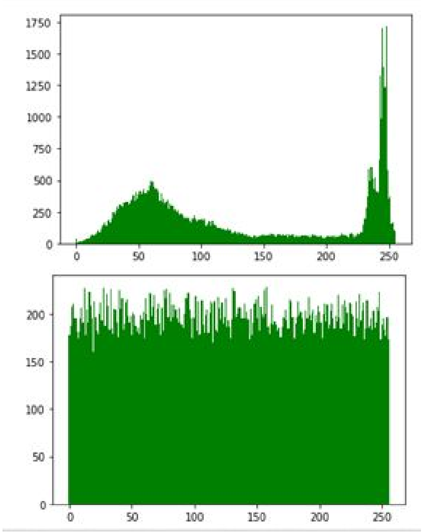
Security Analysis:

Key space analysis –

The secret key X_0 contains a list of 10 secret keys, each with a precision of 10^{-16}. Since the chaotic map changes with a step of 10^{-16}, the key space for the initial condition is $(10^{16})^{10} = 10^{160}$. Furthermore, keys K_C and K_R consist of M and N values where M and N are the width and height of the image respectively. Each value in K_C and K_R is an 8 bit number. Hence the total key space for a 300 x 300 image would be $(2^8)^{300}$ x $(2^8)^{300} = 2^{4800}$. This key space is large enough to resist brute force attacks.

Statistical analysis –

<u>Histogram analysis:</u>



As shown above, the first histogram represents the distribution of pixel values in the original image, and the second histogram represents the distribution of pixel values in the encrypted image. The encrypted image histogram is uniform

Correlation:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i.$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2,$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right).$$

$$\gamma_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{with } D(x) \neq 0,\ D(y) \neq 0.$$

.

- Horizontal Correlation of Original Image = 0.9688906384109065
- Vertical Correlation of Original Image = 0.9636445726326363
- Diagonal Correlation of Original Image = 0.9411261696271439

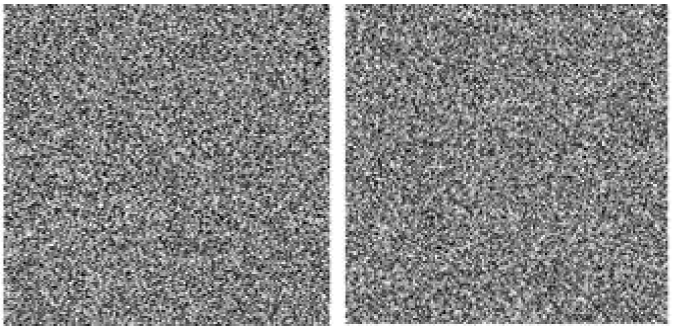
- Horizontal Correlation of Encrypted Image = 0.02403049486257048
- Vertical Correlation of Encrypted Image = 0.0317221978074735
- Diagonal Correlation of Encrypted Image = 0.061165415766847794

As shown in the above values, the correlation between pixels in the original image is very high and the correlation between pixels in the encrypted image is very low.

Differential attack:

$$\mathrm{UACI}_{\mathrm{R,G,B}} = \frac{1}{W \times H}\left[\sum_{i,j}\frac{\left|C_{\mathrm{R,G,B}}(i,j) - C'_{\mathrm{R,G,B}}(i,j)\right|}{255}\right] \times 100\%$$

$$\mathrm{NPCR}_{\mathrm{R,G,B}} = \frac{\sum_{i,j} D_{\mathrm{R,G,B}}(i,j)}{W \times H} \times 100\%$$



The encrypted images above are encrypted versions of images that differ in only one pixel.

Two values, Number of Pixels Changed Rate, and Uniform Average Changed Intensity determine the security of the encryption algorithm. The NPCR should be as close to 100% as possible, and the UACI should be in the vicinity of 33.3% for two encrypted images whose original image differs by only one pixel.

- Number of Pixels Changed Rate = 99.59506172839507%
- Unified Average Changed Intensity = 33.25873638344227%

As shown above, the NPCR and the UACI values are very close to their optimal values.

Applications of Visual Cryptography

Biometric Authentication

Biometrics is the science where the identity of an individual is verified on the basis of their physical traits such as fingerprint, iris, retina, and voice. The system operates by storing the raw data of an individual in the database at the time of enrolment, and this data is processed and then used to verify the identity of the individual when required. As biometric templates are stored in the centralized database, due to security threats biometric templates may be modified by attackers. If the biometric template is altered authorized users will not be allowed to access the resource. To deal with this issue visual cryptography schemes can be applied to secure the fingerprint template. Visual cryptography provides an extra layer of authentication and security.

Increasing Security using Visual Cryptography

The proposed approach is divided in two parts 1.) Enrolment Mode, 2.) Authentication Mode

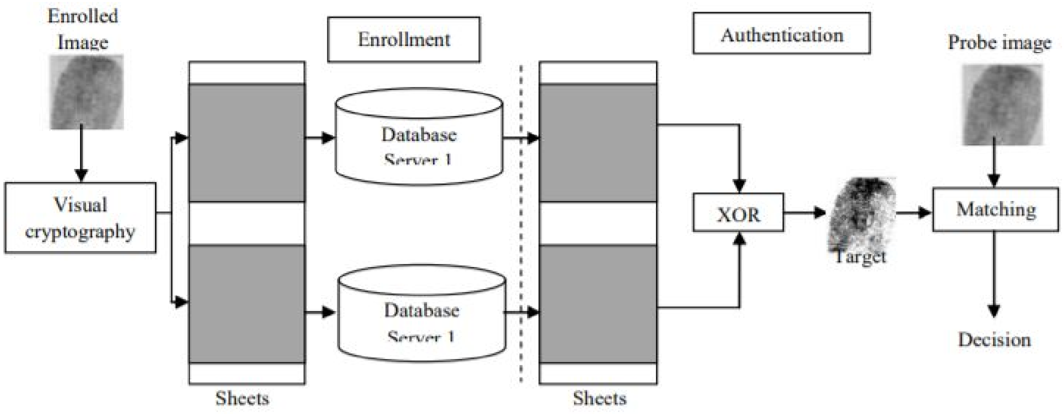
1. **Enrolment Mode**

   The enrolment Mode is the collection or enrolment phase of user data when a user creates an account. The system collects the user data and applies the visual cryptography schemes on the data to make them visually unrecognisable, such that an attacker faces difficulty in decoding the scrambled image. Image scrambling is done by applying the permutation algorithm. Using the key value some permuted sequence will be generated and apply the sequence to the image. The original image can be decomposed into blocks; each one containing a specific number of pixels. These visually encrypted blocks of image will be transferred into the new database as per the permutation algorithm and the original image will be deleted. Now the attacker needs to attack at least k out of n database in order to get the minimum no. of shares required to successfully obtain the original image.

2. **Authentication Mode**

During the authentication process, the trusted entity sends a request to each server and the corresponding shares are transmitted to it. These shares are then superimposed in order to get the final reconstructed image from the scrambled image. An inverse permutation combination is obtained only by using the same key that was used while encryption.

This scheme can be used on the previously encrypted images (AES) also, to increase the level of security, as K no. of images are required to get the original image.



Results for Biometric Authentication

In the project the biometric image of fingerprint was taken and divided into the n shares out of which K were required to attain the image properly. It was observed that as the value of N and K were increased there was an increase in the level of randomness. It was also observed that if K chosen was less than that of specified at the time of encryption, the image had some noise but was somewhat recognizable. This can be removed by first encrypting the image and then applying VCS.

The biometric verification was done using Minutiae recognition. The Image database consisted of 180 fingerprint images with 8 different images of a fingerprint of a single person and a total of 10 different persons. The accuracy of .5 was used for successful identification of a fingerprint. It was observed that all the correct fingerprints had accuracy above .5 while the incorrect ones had accuracy in range of 0.2-0.3. Hence they can be easily differentiated from the true fingerprints image.

Digital image copyright protection

"Good artists imitate, great artists steal" ~ Picasso.

With the rise of technology where everything is going digital, protection of digital intellectual property is fast becoming a prominent issue. The technology for enforcing such protection is advancing rapidly and has already reached commercialization. Digital storage technology and increased availability of high speed internet provide an unprecedented opportunity to make valuable content available to the vast public. With this comes increased threat of abuse and piraacy.

Reasons to use copyright protection schemes:-

1. **Ownership assertion and copyright protection:-** owner should have a way to embed or attach some information to the content so as to establish ownership and to be able to resolve disputes, if necessary.

2. **Fingerprinting:-** To avoid unauthorised duplication and sharing of content owned by a private entity which is available publicly, an invisible can be attached with the content.
3. **Hidden information:-** Some situations demand to embed hidden information like meta-data within the content itself.
4. **Authentication and integrity:-** Legal documents need to be verified if they were tampered or falsified. Digital signatures can be used for this purpose along with the current technology.

Parties involved in this scheme:-

1. Content creators
2. Content users
3. Content providers
4. Graphic software vendors
5. Attackers
6. Manufacturer of equipment

Technology for the protection of Digital images

Digital Watermarks

Paper watermarks have been used for ages when their purpose was to record the trademark of a manufacturer. Modern watermarks are used for the same purpose. A digital watermark is some information added to the image when it is created or packaged for distribution which can be separated later and verified.

Watermarks can both be visible or invisible dependent on the use case. Watermarks can also be designed to be fragile or robust. Fragile watermarks get corrupted with little modification. These are mostly used to detect changes made to the image, if any. Robust watermarks on the other hand are preserved after common manipulations like cropping, resizing, color and brightness modification, etc. These are mostly used for ownership protection.

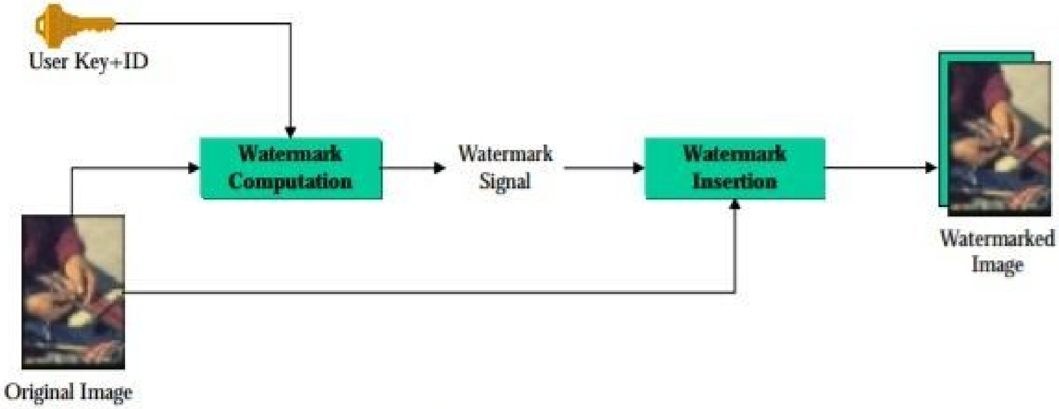


Figure 1 Watermark insertion

General operations involved in watermarking are shown in the figure above. For simplicity we assume watermark to be an image itself which is a function of parameters like user's identity, user's private key, etc. The watermark insertion step combines the watermark with the original image using pixel-by-pixel sum for the simplest case. Depending on the use and type of watermark other combining techniques can be used.

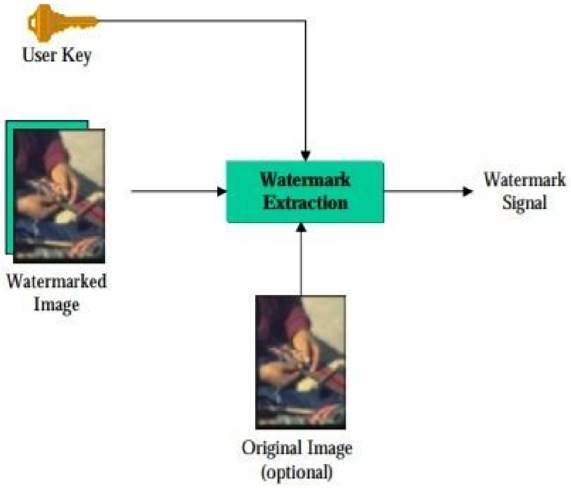


Figure 2 Watermark Extraction

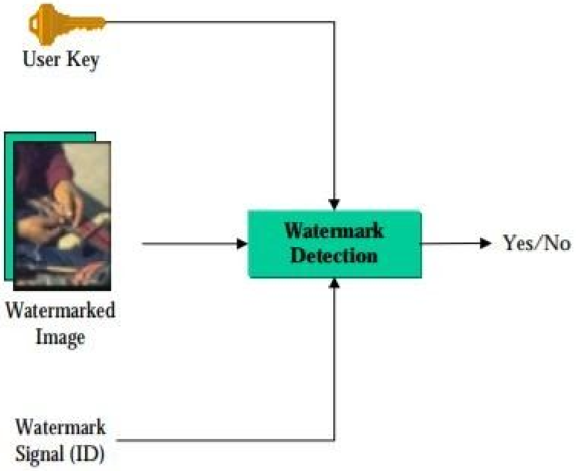


Figure 3 Watermark Detection

The extraction algorithm requires a user key to separate the watermark from the image. Watermark detection also requires that the ID be presented at times. ID can also be one of the parameters while embedding the watermark. This algorithm checks whether there is enough correlation between the input ID and image, returning a value of yes/no depending on the threshold set.

Watermarking techniques like this require a user key which are classified as public or private key. For this a secure transmission channel is also needed for the exchange of keys.

Known Limitations and vulnerability:-

Watermarking technique is not quite old and it's commercial use started just some years back. Since this is not mature technology, the required infrastructure and protocols are almost non-existent. Robust watermarking is still a problem because of its need to survive various manipulations.

Watermark robustness can be attacked both technically and non-technically. Robustness attack attempts to modify the pixel values of the image. They are either based on signal processing algorithms or on the discovery and analysis of insertion and detection algorithms. Software available online have been able to break several commercial watermarking techniques.

Analytic attacks exploit the weaknesses of specific techniques used for watermarking. For example if the detector is available to the attacker, they can use it iteratively to find its behaviour, thus compromising the technique.

A presentation attack doesn't remove the watermark, but manipulates the image such that a detector is not able to detect it. Thus circumventing the copyright protection scheme.

An interpretation attack attempts to neutralize the evidence which is provided by attaching the watermark. For example the attacker may attach their own watermark of equal strength, thus causing ownership ambiguity. Thus watermarking alone are not sufficient to resolve rightful content ownership.

Conclusion

The field of visual cryptography is advancing rapidly and is already being used in commercial applications. In the project we studied and implemented various different techniques and the results obtained were also pretty good. We can confidently say that, it can be used to increase the level of security, But However it's still not mature enough, and there are certain disadvantages like large storage space in comparison to standard techniques. Applications of visual cryptography are immense and need to be further researched to make it commercially viable.

References

- https://www.hindawi.com/journals/scn/2019/8694678/
- https://www.hindawi.com/journals/jece/2012/173931/
- https://scialert.net/fulltext/?doi=jai.2014.123.135#:~:text=Image%20encryption%20can%20be%20defined,users%20can't%20access%20it.
- https://www.sciencedirect.com/science/article/pii/S0898122110001938
- https://www.researchgate.net/publication/261960045_Image_Encryption_Using_Chaotic_Maps_A_Survey
-
- IEEE Transactions on 7, no. 1 (2012): 269-282
- M. Naor, and A. Shamir. Visual Cryptography. Advances in Cryptography-Eurocrypt 1994
- https://www.academia.edu/37354001/Visual_Cryptography_using_KN_Sharing_Algorithm_for_Colour_Images
- An Optimal (k,n) Visual Secret Sharing Scheme for Information Security Mahmoud E. Hodeisha, Linas Bukauskasb, Vikas T. Humbec
- http://datagenetics.com/blog/november32013/index.html
- Argones Rua, Enrique, Emanuele Maiorana, Jose Luis Alba Castro, and Patrizio Campisi. "Biometric template protection using universal background models: An application to online signature." Information Forensics and Security, IEEE Transactions on 7, no. 1 (2012): 269-282
- Ross, Arun, and Asem Othman. "Visual cryptography for biometric privacy."IEEE transactions on information forensics and security 6, no. 1 (2011): 70-81.