DOCUMENT AUTHENTICATION AND VERIFICATION

[1]NAMITA SARODE, [2]RESHMA SHENDGE, [3]KOMAL KANKARIYA, [4]VISHAL KHATAL

[1]K.Wagh Institute of Engineering Education and Research, Department of Computer Engineering, Nashik
[2]K.K.Wagh Institute of Engineering Education and Research, Department of Computer Engineering, Nashik
[3]K.K.Wagh Institute of Engineering Education and Research, Department of Computer Engineering, Nashik
[4]K.K.Wagh Institute of Engineering Education and Research, Department of Computer Engineering, Nashik
Email:namita.sarode@gmail.com, reshmas2207@gmail.com, komalkankariya555@gmail.com, vishkhatal@gmail.com

Abstract— The leading problem in passport, driving license, identity card authentication is to authenticate the document for its owner. The captious factor of this authentication procedure is to establish a correspondence between document's photo and its owner. A document contains holder details in supplement to the holder's signature. We put forth an authentication scheme by extracting some details of the holder including number, name, and other relevant details converting them into a watermark and digesting them in a form by applying some techniques that can be hidden in the photo. The computers have revolutionized the document authentication process by using the computer in fixing the photo on the document during the issuing of document and also verifying the document by scanning it. During the issue of any document, a watermark can be created based on the details of the holder full name and unique number and it can be hidden in the photo on the document using watermarking technique. By using this technique, during the document verification process, computer can be used in scanning the photo to check whether the photo has been replaced by comparing the invisible watermark hidden in the photo with the holder's details including the full name and other relevant details. Because this technique has used only one pixel for hiding the watermark, it satisfied the robustness against image compression.

Keywords— Authentication, Robustness, Steganography, Watermarking

I. INTRODUCTION

1.1 Steganography

Steganography is the art and science of encoding hidden messages in such a way that no one other than the sender and intended recipient, suspects the existence of the message. It is a form of security through equivocation. The word steganography belongs to Greek origin and means "concealed writing". It combines the Greek words steganos means "covered or protected", and graphei means "writing".

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is dealt with concealing the fact that a secret message is being sent, as well as hiding the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications contains steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might begin with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet; a change is so minor that no one can specifically notice it.

1.2 Digital Watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal and there is no relation between hidden information and carrier signal. Digital watermarks can be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is mainly used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and not detectable else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. A signal may carry several different watermarks at the same time. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But steganography aims at imperceptibility to human senses, digital watermarking tries to control the robustness as its higher priority.Since a digital copy of data is the exact copy of original data, digital watermarking is a passive protection tool.

There are certain requirements for Watermarking Techniques:

A. Robustness

The embedded information is said to be robust if its presence can be reliably detected after the image has been modified, but not destroyed beyond recognition.

B.Invisibility

This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carries that contain the hidden information and those that do not.

C.Undetectability

The concept of undetectability is inherently tied to the statistical model of the image source. If an attacker has a more detailed model of the source, he may be able to detect the presence of a hidden image, but this does not imply the ability to read the hidden message.

D.Security

The embedding algorithm is said to be secure, if the embedded information can not remove beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, computer involved in all life details. zne of these issues is producing the document by using the computer application. To fill full this objective there are several requirements such as using a computerize photo for the document holder with special colors (grey and white). Also most of the document offices are connected through a network to exchange their information about the correctness of document information and the authentication of the document holder. It is possible to transfer the image between different offices to get information confirmation.

Here, the main problem is how to confirm and authenticate the document holder's photo with the information about the holder. There is no other way to tell if the photo been replaced with a new one (for the current holder) because there is no physical connection between the photo and the holder’s details.

II. EXISTING SYSTEM

The existing system is based on authentication of passport only. The aim of the existing algorithm is to provide a firm association between the holder’s photo and the holder’s details. The existing algorithm used the watermarking technique to create an association between the photo and holder’s details by embedding hidden information in the photograph. The existing algorithm uses the holder’s first name, second name, third name, family name and document number and converts into an invisible watermark. This invisible watermark is embedded inside the photo such that it satisfies all the requirements of the watermarking technique. This process is carried out during the issue of the document at the office. The existing algorithm consists of three algorithms. The first algorithm deals with acquiring the required parameters for creating the watermarking. The second algorithm converts the holder’s details into a watermark that can be embedded into the digital image. The third algorithm hides the watermark obtained inside the photo such that it meets the requirements of the watermarking.

2.1 Drawbacks

1. Due to rapid advancement in technology, new tools were invented to compare original image and Steganography image to detect the presence of hidden information in a Steganography image.
2. Suppose a Steganography image is created by existing method values of row, Rcolumn can be obtained by Comparing original image with Steganography image.
3. An attacker having the full knowledge of the algorithm, can be able to crack the key value by running a program on super computers by trial and error method.

III. PROPOSED SYSTEM

The proposed system is designed for various documents like employee’s identity, driving license, passport, etc. This system can be used for authentication and verification of any document which contains photo in it. The aim of the proposed method is to develop a firm connection between the photo and the holder's details. In this case it is possible to use this method for confirmation of holder’s information.

The summery of this method is by converting the holder's name (1st, 2nd, 3rd and family name) in addition to the document number is called as invisible watermark. This watermark will be hide and distributed inside the photo. This process will be done during the issue of the document for the first time. All the watermark requirements will be considered. The proposed method contains several algorithms. All the required method is used for authentication nad verification. The following algorithms are used in the proposed method. In consideration we have considered passport document :

3.1. Algorithm 1: Acquire Parameters

1. Get holder’s first name, second name, third name and surname.
2. Generate holder’s document Number unique to each user.
3. Validate the holder’s details.
4. Assign a number to each letter of the name according to the table 1.
5. Store each name’s numbers for future reference

3.2. Algorithm 2: Watermark

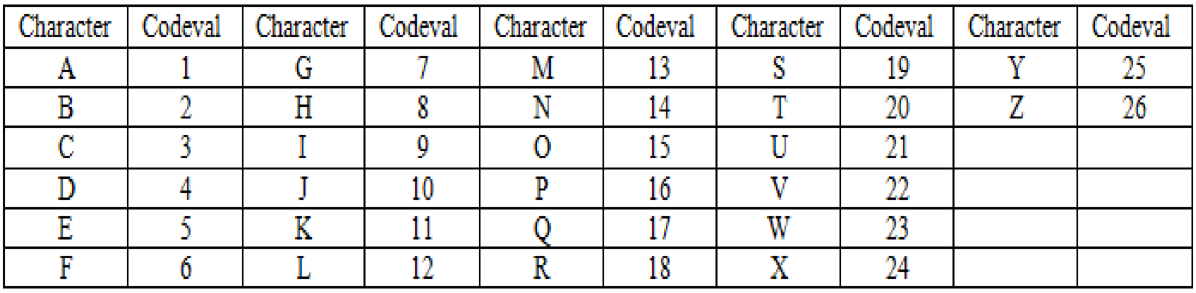
1. Consider the key value. E.g. K = "1, 2, 3, 4".
2. Create a new key value for first name by summing the consecutive key values in a round robin fashion say K1.

Where K1(1)=K(1)+K(2)
K1(2)=K(2)+K(3)
K1(3)=K(3)+K(4)
K1(4)=K(4)+K(1)

Compute the summation of the first name by adding the code value consider values from from table 1of each character multiplied by the new key’s character in succession.

E.g. codeval(1)*K1(1) + codeval(2)*K1(2) + codeval(3)*K1(3)+……

3. Consider the result as "row”.



Character	Codeval	Character	Codeval	Character	Codeval	Character	Codeval	Character	Codeval
A	1	G	7	M	13	S	19	Y	25
B	2	H	8	N	14	T	20	Z	26
C	3	I	9	O	15	U	21		
D	4	J	10	P	16	V	22		
E	5	K	11	Q	17	W	23		
F	6	L	12	R	18	X	24		

Table 1.Alphabets and their corresponding codevalue

4. Create a new key value for second name by summing the alternate key values in round robin fashion say K2.
 Where K2(1)=K(1)+K(3)
 K2(2)=K(2)+K(4)
 K2(3)=K(3)+K(1)
 K2(4)=K(4)+K(2)
 Compute the summation of the second name by adding the code value of each character multiplied by the new key's character in succession.
 E.g. codeval(1)*K2(1) + codeval(2)*K2(2) + codeval(3)*K2(3)+…….
5. Consider the result as "column ".
6. Compute the summation of the third name and family
 name by adding the code value of each character
 multiplied by the actual key's character in succession.
 E.g. codeval(1)*K(1) + codeval(2)*K(2) + codeval(3)*K(3)+……
7. Compute the summation of document number by adding
 the code value of each character.
 E.g. codeval(1) +codeval(2)+ codeval(3)+……
8. Compute the sum of third name, family name and the
 Document number and store the result in "sum".

3.3. Algorithm 3: Hide Watermark

1. Get the pixel value at (row, column) location from the original Image.
2. Find the average value of RGB [6] color for that pixel,
 add 1 to it and assign it to "avg ".
3. Divide "sum" on "avg" to get number of pixels.
4. Compute the modulo division of "sum" over "avg" and store result in "value ".
5. Calculate Rcolumn which is equal to "column" + "number of pixel" + 1.
6. Get the pixel value at location (row, Rcolumn).
7. Get the largest value of (R,G,B) for the pixel at that location and replace it with "value".
8. Restore the pixel (R,G,B) values at the same location.
 otherwise take legal proceedings on the passport holder.

3.4. Algorithm 4: LSB Algorithm

This approach [5][6] is very simple. In this algorithm, least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. This paper tries to cover the disadvantages of LSB algorithm. While computing, the least significant bit (LSB), the bit position in a binary integer giving the units value i.e. determining whether the number is even or odd. It is sometimes referred as Left-Most Bit because of the convention in positional notation of writing least significant digits further to the right. In referencing specific bits within a binary number, it is common to assign each bit a bit number, ranging from zero upwards to one less than the number of bits in the number. However, the order used for this assignment may be in either direction. Both orderings are used (in different contexts), which is why "LSB" is often used to designate the units bit instead of a bit number, which has the potential for confusion. By extension, the least significant bits (plural) are the bits of the number closest to, and including, the lsb. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000). Least significant bits are frequently employed in pseudorandom number generators, hash functions and checksums.LSB, in all capitals, can also stand for "Least Significant Byte". The meaning is parallel to the above: it is the byte (or octet) in that position of a multi-byte number which has the least potential value.

IV. ANALYSIS

Algorithm one will accept the passport holder full Name and generates a unique number such as passport number of employee's ID number for the creation of watermark, which is validated to make sure that all the given information is correct.

Each letter in Full name is assigned a codeval chosen from table 1.this table contains the alphabets and their equivalent numbers. The following equation can be used to compute the code value for each character.

Codeval (character)=ASCII value(character)-64.

By the end of each algorithm one each name (first, second, third and surname)has a sequence of numbers assigned to each name depending on the length of name.

Algorithm two starts by selecting a kay K(e.g 1,2,3,4) and then calculating the key value for each name according to algorithm as follows:

For First name, a separate key value is calculated (say K1)

As

K1(1)=K(0)+K(1)
K1(2)=K(1)+K(2)
K1(3)=K(2)+K(3)
…………………………………

For Second name, a separate key value is calculated (say K2)

As

K2(1)=K(0)+K(2)
K2(2)=K(1)+K(3)
…………………………………

For Third name, actual key value is taken into consideration then the value for each name is calculated by multiplying code value for each character by corresponding key digits arranged in sequence and summing up the values.

For the passport number each number each digit is converted to a code value and is summed in sequence.

e.g. codeval(1)*K1(1) + codeval(2)*K1(2) +
codeval(3)*K1(3)+……for first name
codeval(1)*K2(1) + codeval(2)*K2(2) +
codeval(3)*K2(3)+……for second name
codeval(1)*K(1) + codeval(2)*K(2) +
codeval(3)*K(3)+……for third name,surname.
Pno(1)+pno(2)+……..for unique number

The following equations can be used to calculate value for each name

J=m
I=n
Σcodeval(i)*K(j)
I=1
J=1

Where, n=length of name and m= length of key. And K refers to K1 for first name, K2 for second name and K for third name and surname.

Suppose first name is JAGADEESH
Second name is KUMAR
Third name is RAJU
surname is POTLURI
Passport number is HYD44444
Actual Key value is 1234
Value of JAGADEESH is row=280
Value of KUMAR is column=300
Value of RAJU is 134
Value of POTLURI is 238

After we divide the "sum" on "avg" to obtain the number of pixels. We use modulo of "sum" over "avg" to get "value". Then we calculate the new column for the pixel to be hidden i.e. Rcolumn as column number of pixels + 1. Then value of max(R,G,B) for pixel(row, column) is replaced with value.

Improved algorithm has an advantage over existing algorithm in terms of security. The improved algorithm uses different keys for first name, second name and third name, family name which does not allow intruder to crack key given the full knowledge of algorithm. So it satisfies the security requirement of watermarking. Also improved algorithm overcomes the divide by zero exception that may occur in the existing algorithm by adding positive quantity (1) to the avg. So the improved algorithm overcomes the drawbacks of the existing algorithm.

CONCLUSION

This authentication scheme embeds the invisible watermark into the photo to authenticate the document owner. This modified scheme meets all the requirements for the watermark technique. This method is effective and meets all the requirements of watermarking. The invisible watermark has satisfied the robustness, Invisibility, Undetectability and Security requirements. Because this technique has used only one pixel for hiding the watermark, it satisfied the robustness property. The detection of presence of hidden information is a difficult task as it is time consuming to predict the key value. So it satisfies the security requirement of watermarking. It also satisfies invisibility requirement because change in one pixel is not visible to the human eye.

The watermark also satisfies the Undetectability requirement since the pixel size is very small compared to the size of an image and is not easily noticeable. This scheme is applicable for only one State. So to make the authentication scheme globally feasible, every state should share keys using asymmetric key cryptography. Every state should use the public key to hide the watermark during the issue of any document and private key should be used during the verification process at the checkpoint to check the authenticity of a document.

REFERENCES

[1] AlaaH.Al-Hamami and SaadA.Al-Ani, Faculty of Information Technology, Amman Al-Ahliyya University, Amman, Jordan “A New Approach for Authentication Technique”Journal of ComputerScience 1 (1): 103-106, 2005 ISSN 1549-3636 © Science Publications, 2005

[2] ManjitThapa, Dr.Sandeep Kumar Sood, A.P Meenakshi Sharma “Digital Image Watermarking Technique Based on Different Attacks”. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011.

[3] Christian S. Collberg, Member, IEEE Computer Society, and Clark Thomborson, Senior Member, IEEE “Watermarking, Tamper-Proofing, and Obfuscation Tools for Software Protection” IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 28, NO. 8, AUGUST 2002.

[4] Rafael C. Gonzalez and Richard E. Woods, 2001 “Digital image processing”, second edition ISBN 0-201-18075-8Prentice hall publications.

[5]Bender, W., D. Gruhl, and N. Morimoto, “Techniques for data hiding”, IBM Systems Journal , vol. 35, no. 3/4, 1996, pp. 131-336.

[6] Moller. S.A., Pitzmann, and I. Stirand, “Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best”, in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 7-21.

[7] Stefan, K. and F.A.P. Petitcolas (Eds.), 2000. Information Hiding techniques for steganography and digital watermarking. ISBN 1-58053-035-4 © Artech House, Inc.

★★★