ISSN 2250-3153

Visual Cryptography Using Two Factor Biometric System for Trust worthy Authentication

Mrs. A. Vinodhini, M. Premanand, M. Natarajan

G.K.M College of Engineering and Technology
Perungalathur, Chennai-600063

Abstract- Authenticity of the user is the major issue in today's internet applications such as online transaction. Password has been the most used authentication mechanism which is subjected to online attacks. Due to unavoidable hacking on the internet, it is difficult to trust the User Identity on the internet. To solve this problem this paper proposes a BIOMETRIC based Visual Cryptography scheme to address the authentication issues. This methodology proposes the finger print image which is obtained from the user is Steganographed with PIN NUMBER of the user and the Steganographed image which in turn is divided into two shares. One share is stored in the bank database and the other share is provided to the customer. Hash code is generated for the customer share and it is stored in the bank database. One Time Password(OTP) is used every time to ensure the trusted submission of shares. The system not only ensures the secured transaction of process but also verifies the true identity of the person through one time password. The customer has to present the share during all of his/her transactions after entering the OTP. When the customer presents his share the hash code is generated and compared with the database value. If it matches, the shares are stacked to get the original Steganographed image. Again, the Desteganography process is carried on to obtain the original finger print image and the PIN NUMBER. The user is allowed to proceed further only after this authentication. This process ensures proper security scheme.

Index Terms- Visual Cryptography, authentication issues, finger print image, steganographed image

I. INTRODUCTION

Trusting User Identity on the internet is quite difficult due to hacking of User identity on the internet. So it is nearly impossible to be sure whether a user connected to the internet is authenticated or not. In Online transaction there is a possibility of encountering forged Identity for transaction. In the Online transaction system, the password of the customer may be hacked and misused. This paper proposes a technique to improve security during transaction. An idea based on Steganography and Visual Cryptography is used. Visual Cryptography introduced by Naor and Shamir [1] is a method used for encrypting a secret image into shares, such that stacking the shares reveals the secret image. The main advantage of Visual Cryptography is the decryption of the message which does not involve more process. The decryption time is very less when Visual Cryptography technique is used. Visual Cryptography is used to check a person for his/her authentication.

Visual Cryptography provides a very powerful technique by which one secret can be distributed in two or more shares. When the shares on transparencies are superimposed exactly together the original secret can be discovered without computer participation.

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioral traits such as face, fingerprints, iris, gait, and voice. A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., thumb impression), extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography can be applied to different types of media including text, audio, image, video, etc. However, text steganography is considered to be the most difficult kind of steganography due to the lack of redundancy in text as compared to image or audio

One Time Password uses information sent in an SMS to the user as part of the login process. One scenario is where a user either registers (or updates) their contact information on a website. During this time the user is also asked to enter his or her regularly used telephone numbers (home, mobile, work, etc). The next time the user logs in to the website, they must enter their username and password; if they enter the correct information, the user then chooses the phone number at which they can be contacted immediately from their previously registered phone numbers. The user will be instantly called or receive an SMS text message with a unique, temporary PIN code. The user then enters this code into the website to prove their identity, and if the PIN code entered is correct, the user will be granted access to their account

A hash function is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes.

In cryptography, SHA-1 (Secure Hashing Algorithm) is a widely used cryptographic hash function with a 160-bit hash value. As an Internet standard (RFC 3174), In theory no two messages would ever share the same message digest. What this

means is that the message digest can serve as a fingerprint for a file or other source of data. SHA-1 is used by Digital Signature Standard (DSS), which is a standard used for digitally signing documents or other data.

II. RELATED WORK

This section provides a brief description of Visual Cryptography and its applications. Although introduced and studied in the late 1970's and early 1979's Visual Cryptography have become increasingly popular in the last several years. Visual Cryptography schemes were independently introduced by Shamir[2] and Blakely[3].

In Visual Cryptography each pixel appears in n modified shares. The shares are a collection of m black and white sub pixels arranged closely together. This is described as an n x m Boolean matrix. When the shares are superimposed and the sub pixels are correctly aligned the original image is obtained. Since the individual shares gives no idea of whether a specific pixel is black or white it become impossible to decrypt the shares, no matter how much computational power is available.

Visual Cryptography scheme (VCS) proposed by Feng Liu and ChuanKunWu [4] can be applied to avoid largest pixel expansion. This paper gives details about the (2; n) VCSXOR can achieve smaller pixel expansion and larger contrast than that of (2; n) VCSOR.

Visual Cryptography scheme introduced by Naor and Shamir, explains about secret sharing. Secret sharing is an algorithm in cryptography where a secret is divided into n parts, giving each participants a unique part, where some of the parts or all of them are needed to reconstruct the secret.

A segment based Visual cryptography proposed by Jithesh, Dr. A. V. Senthil Kumar [5] used blend steaganography and visual cryptography. Steganography and Visual Cryptography are two sides of a coin. Visual cryptography has the problem of revealing the existence of the hidden data where as Steganography hides the existence of hidden data

Visual Cryptography scheme proposed by W-QYan et al., [6] can be applied only for printed text or image. The shares of Visual Cryptography are printed on transparencies which need to be superimposed. A Visual Cryptography method proposed by T.Monoth et al.,[7] uses random basis column pixel expansion technique. The encoded shares are further encoded into number of sub shares recursively which is computationally complex. Similarly a technique proposed by H.J.Kim et al., [8] explains an algorithm for secret sharing scheme that allows a group of participants to share a secret among them. In this paper we propose a Visual Cryptography scheme based on BIOMETRIC image. Shares are created for the steganographed thumb image generated using the pin number.(2,2) Visual Cryptography is used to create the shares. One share is in the server database and the other is with the user. When shares are superimposed , original steganographed thumb image is recovered which is further desteganographed to split the the thumb image and PIN Number which authenticates the user.

III. ARCHITECTURE AND MODELLING

Visual cryptography is a cryptographic technique Which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers).

It involves breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. In this technique n-1 shares reveals no information about the original image. We can achieve this by using one of following access structure schemes [8].

1:(2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2 :(2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed.

3 :(n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined the secret image will be revealed.

4:(k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

Basic visual cryptography is based on breaking of pixels into some sub pixels or we can say expansion of pixels. There are two approaches for (2, 2) –Threshold VCS. In this first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel BT+TB=BB or TB+BT=BB and for white pixel BT+BT=TT or TB+TB=TT. Similarly second approach is given where each pixel is broken into four sub pixels. We can achieve 4C2 =6 different cases for this approach.[8].

The model for creating shares[9] is explained here.

Let P = {1,..., n} be a set of elements called *participants*, and let 2^P denote the set of all subsets of P. Let $\Gamma_{Qual} \subset 2^P$ and $\Gamma_{Forb} \subset 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. The members of Γ_{Qual} are *qualified sets* and members of Γ_{Forb} are *forbidden sets*. The pair (Γ_{Qual}, Γ_{Forb}) is called the *access structure* of the scheme.

Let Γ_0 consists of all the minimal qualified sets:

$\Gamma_0 = \{A \in \Gamma_{Qual} : A' \notin \Gamma_{Qual} \text{ for all } A' \subset A\}$.

A participant $P \in P$ is an essential participant if there exists a set $X \subset P$ such that $X \cup \{P\} \in \Gamma_{Qual}$ but $X \notin \Gamma_{Qual}$. If a participant P is not essential then we can construct a visual cryptography scheme giving him a share completely white or even nothing as his share. In fact, a non-essential participant does not need to participate actively in the reconstruction of the image since the information he has is not needed by any set in P in order to recover the shared image. In any VCS having non-essential participants, these participants do not require any information in their shares. We assume all participants as essential.

In the case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$, the access structure is said to be strong, and Γ_0 is termed a basis. In a strong access structure,

$\Gamma_{Qual} = \{C \subset P : B \subset C \text{ for some } B \in \Gamma_0\}$,

and we say that $\overline{\Gamma}_{Qual}$ is the closure of Γ_0 .

We assume that the message consists of black and white pixels. Each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white subpixels. The resulting structure can be described by an n x m Boolean matrix S=[s_{ij}] where s_{ij}=1 iff the j th subpixel in the ith transparency is black. Therefore the grey level of the combined share, obtained by stacking the transparencies i_1, ..., i_s, is proportional to the Hamming weight w(V) of the m-vector V=XOR($r_{i1,\ldots,}r_{is}$) where r_{i1} , ..., r_{is} are the rows of S associated with the transparencies we stack. This grey level is interpreted by the visual system of the users as black or as white in according with some rule of contrast.

Definition: Let (Γ_{Qual}, Γ_{Forb}) be an access structure on a set of n participants. Two collections (multisets) of nxm boolean matrices b_0 and b_1 constitute a visual cryptography scheme (Γ_{Qual}, Γ_{Forb}, m)-VCS if there exist the value α(m) and the set $\{(X, t_X)\}x\epsilon\ \Gamma_{Qual}$ satisfying:

1. Any (qualified) set X= {i1, i2, ..., ip} $X\epsilon\ \Gamma_{Qual}$ can recover the shared image by stacking their transparencies. Formally, for any M ϵ b_0, the "or" V of rows i1, i2, ..., ip satisfies $w(V) \leq t_x - \alpha(m).m$; whereas, for any M ϵ b_1 it results that $w(V) \geq t_x$.
2. Any (forbidden) set X= $\{i_1, i_2, \ldots, i_p\} \epsilon\ \Gamma_{Forb}$ has no information on the shared image. Formally, the two collections of p x m matrices Dt , with t ϵ {0, 1}, obtained by restricting each n x m matrix in b_t to rows i_1 , i_2 , ..., i_p are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Each pixel of the original image will be encoded into n pixels, each of which consists of m subpixels. To share a white (black, resp.) pixel, we randomly choose one of the matrices in b_0 (b_1 , resp.), and distribute row i to participant i. The chosen matrix defines the m subpixels in each of the n transparencies. Notice that in the previous definition b_0(b_1) is a multiset of n x m Boolean matrices, therefore we allow a matrix to appear more than once in b_0 (b_1). Finally, observe that the sizes of the collections b_0 and b_1 do not need to be the same.

The first property is related to the contrast of the image. It states that when a qualified set of users stack their transparencies they can correctly recover the shared image. The value α(m) is called relative difference, the number α(m) .m is referred to as the contrast of the image, the set $\{(X, t_X)\}_{X\ \epsilon\ \Gamma Qual}$ is called the set of thresholds, and t_X is the threshold associated with X $\epsilon\ \Gamma_{Qual}$. We want the contrast to be as large as possible and at least one, that is, α(m)≥1/m. The second property is called security, since it implies that, even by inspecting all their shares, a forbidden set of participants cannot gain any information useful in deciding whether the shared pixel was white or black.

2 out of 2 Scheme : (2 sub pixels)

In Black and white image each pixel is divided into two sub-pixels. Randomly pixels are chosen between black and white. If white, then randomly choose one of the two rows for white.

Pixel		Share 1	Share 2	Result
	P = ½			
	P = ½			

If black, then randomly choose between one of the two rows for black.

Pixel		Share 1	Share 2	Result
	P = ½			
	P = ½			

IV. OUR WORK

Overview of this paper consists of five processes.

1. Obtaining the Thumb Image
2. Steganographing the PIN number
3. Share creation process.
4. Hash code generation
5. Authentication process.

A. Obtaining the Thumb Image

During the creation of new account a user need to provide all his/her details. In addition to this we obtain the thumb image of the user which is the unique identification each user that has been stored in the database. The obtained thumb image is used for the further process.

Fig. 1Thumb Image

B. Steganographing the Pin Number

Steganography is art of hiding information inside information. In our process the pin number of the user is hidden into the user thumb image which avoids the weak links of the bio-metric system.

Fig. 2 Steganographed Thumb image

C. Share Creation Process

Overview of share creation process is shown in Figure 4.3.User registers to the server by providing their details such as Name, Date of birth, Occupation Address and Thumb image which will be stored in the server database. The secret pin number of the user is Steganographed with the thumb image. The generated Steganographed thumb image is divided into two shares. One share is stored in the server database and for the other share Hash code is generated and stored in the database. After that the share is given to the customer.

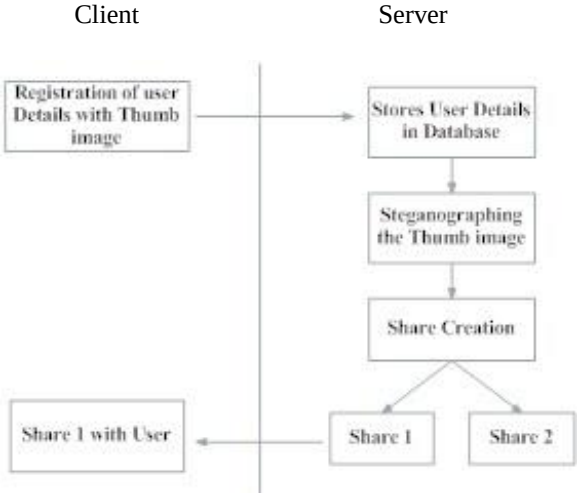
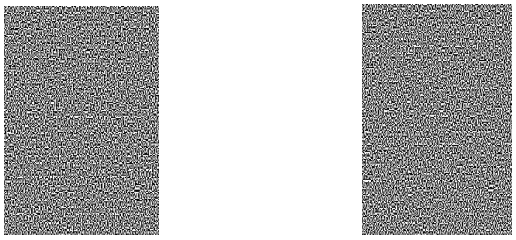


Fig. 3 Share Creation

i. Creation of Shares

The basic assumption here is that the thumb image is a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in *n* modified versions, one for each share. Each share is a collection of *m* black and white sub-pixels that are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. The resulting structure can be described by an *nxm* Boolean matrix S = [sij] where sij =1 iff the j th sub-pixel in the i th share is black. Sij=0 iff the j th subpixel in the i th share is white. Figure 4.3 shows the shares of a image.



(a) Share1 (b) Share2

Fig. 4 Two shares obtained for a image in 2 out of 2 Scheme.

The algorithm for creation of shares is the BIOMETRIC image is converted to its Boolean matrix values. This matrix shows the black pixel and white pixel of the BIOMETRIC image. Initialize the S_0 matrix value and S_1 matrix values in which S_0 shows white pixel and S_1 shows black pixel.

$$S_0 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

$$S_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

If the image value is white then, put the values of first row of S_0 to share1 and second row of S_0 to share2.Similarly continue for all pixels of the BIOMETRIC image. So each pixel is represented using four subpixels which represent two shares. Thus the (2, 2) shares are generated

D. Hash Code Generation

Hashing is a process which includes the conversion of the Crypto graphed image into the hash code bytes. This conversion is done by using SHA-1 algorithm. Where SHA stands for Secure Hashing Algorithm. SHA-1 is a widely used cryptographic hash function with a 160-bit hash value. As an Internet standard (RFC 3174). SHA-1 uses output size and internal state size of 160bits. The block size is of 512 bits. The maximum message size for for an SHA-1 algorithm is 2^64-1 bits. Word size is of 32 bits and 80 rounds. The operations are add, and, OR , XOR.

E. Authentication Process

When the customer types the One Time Password and enters into the system to presents his/her share for Online Bank Transaction, Hash code is generated for that share and compared with the hash code in the database. If it matches then further process carried out by reconstructing the shares to obtain the original steganographed image and desteganography process is carried on to reveal the original pin number and thumb image. It verifies the authentication of the true person.

i. One Time Password (OTP)

An One Time Password is generated to ensure the true identity of the person before the user gives the the share. When user login to the system for a transaction an One Time Password is sent to his/her mobile when the user enters the OTP he/she allowed for the further process else the process truncated.

ii. Stacking

The original image is reconstructed by stacking the transparencies[1]. When transparencies i1 , i2,…., ir are stacked together in a way which properly aligns the sub-pixels, one can see a combined share whose black sub-pixels are represented by the Boolean X*OR* of rows i1, i2 , …., ir in *S*.

- The grey level of the combined share is interpreted by the visual system:
  1. as black if $H(V) \geq d$
  2. as white if $H(V) < d - \alpha m$
- $1 \leq d \leq m$ is some fixed threshold and $\alpha > 0$ Is the relative difference.
- H(V) is the hamming weight of the " XOR " Combined share vector of rows $i_1,\ldots i_n$ in S vector.

When we are stacking the shares the following procedure is followed for each subpixels of share1 and share2. If the value of share1 is black then have the value as 1 in an output matrix1.If the value of share1 is white then have the value as 0 in an output matrix1.Do the process for share2 in output

matrix2.Finally XOR the output matrix1 and matrix2 which gives the original image.

V. CONCLUSION

In this paper TWO FACTOR BIOMETRIC system based Visual Cryptography scheme for secure authentication in online transaction has been proposed. Earlier approaches use the signature of the customer for creation of shares. This involves manual intervention and the integrity of the user is not ensured. This approach is efficient by utilizing the BIOMETRIC image from the user and steganographing it with pin number. As the amount of data to be stored in the database increases, the risks associated with database misuse increases. As a result, the issue of database security and integrity continues to cause several challenges and it is necessary that further research be conducted in this direction and using a separate gateway to send OTP.

REFERENCES

[1] M. Naor and A. Shamir, .Visual Cryptography,. *Advances in Cryptography-EUROCRYPT'94*, Lecture Notes in Computer Science 950,1995, pp. 1-12.

[2] A.Shamir,.Howto Share a Secret,. *Communication ACM*, vol. 22,1979, pp. 612-613.

[3] G. R. Blakley, .Safeguarding Cryptographic Keys,. *Proceedings of AFIPS Conference*, vol. 48, 1970, pp. 313-317.

[4] Feng Liu and ChuanKunWu, Optimal XOR based (2,n)-Visual Cryptography Schemes.

[5] Jithesh, Dr. A. V. Senthil Kumar Multilayer information hiding – A blend of steganography and Visual Cryptography.

[6] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. *IEEE Transactions*, ISCAS-2004, pp.572-575.

[7] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,. in *Proceedings of IEEEInternational Conference on Information Technology*, 2007, pp.4143.

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129, No. 2, (1996), pp. 86-106

[9] L. A. MacPherson, "Grey level visual cryptography for general access structures," M.S. thesis, University of Waterloo, Ontario, Canada, 2002.

[10] N. K. Ratha, J. H. Connell, R. M. Bolle Enhancing security and privacy in biometrics – based authentication systems.

AUTHORS

First Author – Mrs.A.Vinodhini, Assistant Professor, G.K.M College of Engineering and Technology, Perungalathur, Chennai-600063, email:vino.aug@gmail.com

Second Author – M.Premanand, G.K.M College of Engineering and Technology,Prungalathur,Chennai-600063, prem.murugann@gmail.com

Third Author – M.Natarajan, G.K.M College of Engineering and Technology,Perungalathur,Chennai-600063,
email :natraj.muralidharan@gmail.