A Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques

A B Rajendra[1] and H S Sheshadri[2]
[1]*IS & E Department, Vidyavardhaka College of Engineering, Mysore - 570002, Karnataka, India*
[2]*E & C Department, PES College of Engineering, Mandya-571401, Karnataka, India*
[1]rajendraab@hotmail.com, [2]hssheshadri@hotmail.com

***Abstract* - Visual Secret sharing schemes (VSSS) and biometrics have been identified as the two most important aspects of digital security. VSSS uses the human visual system to perform the decryption. A VSSS allows confidential messages to be encrypted into k-out-of-n secret sharing schemes. Whenever the number of participants from the group (n) is greater than or equal to the threshold value (k), the confidential message can be obtained by these participants. VSSS is interesting because decryption can be done with no prior knowledge of cryptography and can be performed without any complex cryptographic Algorithms. Based on this study, a new approach to analyze VSSS that uses biometric approach is given in this paper.**

***Keywords* - Visual Cryptography, Visual Secret Sharing**

1. Introduction

There is an increasing dependence on computers at all levels of our life wherein, personal and sensitive information is beingstored and transmitted using computer systems and networks every day. This revolution, however, has brought with it new threats and computer crimes as noticed in the increased number of computer attacks and break-ins. Replicating important information will give greater chance to intruders to access it. On the other hand, having only one copy of this information means that if this copy is destroyed there is no way to retrieve it. Thus, there is a great need to handle information in a secure and reliable way.

During analysis of information processing and management tasks, at least two important questions related thereto may be defined. The first is the gathering and storage of secret information used in specific companies, institutions, or banks. In the recent years this question was intensely developed, and there are many dedicated systems for intelligent semantic querying for selected information as well as systems for archiving such data according to a variety of semantic information. Some databases may include information of special importance or sensitivity, e.g. of strategic data. Therefore, it is worth to focus our attention to the other significant question related to intelligent information management. It is the question of the capacity to ensure secrecy and selective access to such data for the authorized persons. As such data is ever more often stored in digital form; it becomes necessary to design new solutions and algorithms that allow sharing of crucial information between appropriately authorized persons. Such a potential of managing strategic information may be acquired thanks to the use of certain mathematical techniques, originating from the fields of cryptography

In such situations, secret sharing is of great relevance. The basic idea of secret sharing is to divide the information into pieces, so that qualified subsets of these pieces (shares) can be used to recover the secret. Intruders need to get access to several shares to retrieve the complete information. Similarly, they need to destroy several shares to destroy the whole information. The concept of secret sharing was independently introduced by Shamir [1]. Secret sharing becomes indispensable whenever secret information needs to be kept collectively by a group of participants in such a way that only a qualified subgroup is able to reconstruct the secret. An example of such a scheme is a k-out-of-n threshold secret sharing in which there are n participants holding their shares of the secret and every k ($k \leq n$) participants can collectively recreate the secret while any k-1 participants cannot get any information about the secret. The need for secret sharing arises if the storage system is not reliable and secure. Secret sharing is also useful if the owner of the secret does not trust any single person [3]. This concept was first applied to numbers, but in the 1994 researchers extended this concept to images. Visual cryptography is one such method which implements secret sharing for images [2].

The biometrics technology brings a new dimension to individual identity verification [6]. It provides a guaranteed level of accuracy and consistency over traditional methods. Biometrics means "the statistical analysis of biological observations and phenomena". It refers to the use of distinctive physical (e.g., fingerprints, face, retina, iris, hand geometry, palm) and behavioral (e.g., gait, signature, speech) characteristics for automatically recognizing individuals [7]. For VSSS, if it makes use of biometric authentication it will provide more security.

II. Classic Secret Sharing

An algorithm for splitting and sharing secret information is an young branch of cryptography. In the most general case, their objective is to generate such parts for the data in question that could be shared by multiple authorized persons. What arises here is the problem of splitting information in a manner allowing its reconstruction by a certain n-person group interested in the reconstruction of the split information. Algorithm solutions developed to achieve this objective should at the same time make sure that none of the groups of participants in such a protocol, whose number is lesser than the required m persons, could not read the split message. The

algorithms for dividing information make it possible to split it into chunks known as shadows that are later distributed among the participants of the protocol so that the shares of certain subsets of users, when combined together, are capable of reconstructing the original information. There are two groups of algorithms for dividing information, namely, secret splitting and secret sharing [4].

In the first technique, information is distributed among the participants of the protocol, and all the participants are required to put together their parts to have it reconstructed. A more universal method of splitting information is the latter method, i.e. secret sharing. In this case, the message is also distributed among the participants of the protocol, yet to have it reconstructed it is enough to have a certain number of constituent shares defined while building the scheme. The other types of splitting techniques are the methods for information sharing. They are information distribution methods that are somewhat more complex. The algorithms for information sharing are also known as threshold schemes. Using such a scheme allows taking any information and splitting it into n discretional parts known as shares. In such a manner that any m (where m≤n) from among them may be used to reconstruct the information. This is the so-called (m, n)-threshold scheme [9].

III. Visual Secret Sharing Schemes

VSSS proposed by Naor and Shamir [2], is one of the cryptographic methods to share secret images. A VSSS for a set P of n participants is a method to encode a secret image (SI) into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can visually recover the SI, but other, forbidden sets of participants have no information on the SI. A 'visual recovery' of the qualified set X means that they can see the SI by Xeroxing the shares given to the participants in X onto transparencies and then stacking them. Thus, the participants in a qualified set X will be able to see the SI without any knowledge of cryptography and without performing any Cryptographic Computation [5].

The VSSS describes the way in which an image is encrypted and decrypted. There are different types of VSSS.For example, there is the k-out-of-n scheme that says n shares will have to be produced to encrypt an image, and k shares must be stacked to decrypt the image. If the number of shares stacked is less than k, the original image is not revealed. The other schemes are 2-out-of-n and n-out-of-n VSSS. In the 2-out-of-n scheme n shares will be produced to encrypt an image, and any two shares must be stacked to decrypt the image. In the n-out-of-n scheme, n shares will be produced to encrypt an image, and n shares must be stacked to decrypt the image. If the number of shares stacked is less than n, the original image is not revealed. Increasing the number of shares or participants will automatically increase the level of security of the encrypted message [15].In this section, 2-out-of-n scheme is analyzed with its model, basic theory and result.

A. The model

Let P = {1, 2… n} be a set of elements called participants and let 2^P denote the collection of all subsets of P. Let $\Gamma_Q \subseteq 2^P$ and $\Gamma F \subseteq 2^P$, where $\Gamma_Q \cap \Gamma_F = \theta$ .The members of Γ_Q are called qualified sets and members of ΓF are called forbidden sets. The pair (Γ_Q, Γ_F) is called the access structure of the scheme.

Define Γ_O which consist of all minimal qualified sets:

$\Gamma_O = \{A \in \Gamma_Q : A | \notin \Gamma_Q \text{ for all } A^1 \subset A\}$

The message (secret data) consists of a collection of black and white pixels. Each pixel appears in n version called shares, one for each transparency. Each share is a collection of m black and white sub pixels. The resulting structure can be described by an nx m Boolean matrix $S = [s_{ij}]$, where

Sij = 0 ⇔ the j^{th} sub pixel in the ith share is black.

Sij = 1 ⇔ the j^{th} sub pixel in the ith share is white.

Let (Γ_Q, Γ_F) be an access structure on a set of n participants. A $(\Gamma_Q, \Gamma_F, \alpha)$ - VCS with the relative difference α and set of thresholds $1 \leq d \leq m$ is realized using the two n x m basis matrices S^0 and S^1 if the following two conditions hold:

(1) If $X = \{i_1, i_2 \ldots ip\} \in \Gamma_Q$, then the "or" V of rows $i_1, i_2 \ldots i_p$ of S^0 satisfies $H(V) \leq d - \alpha .m$; whereas, for S^1 it results that $H(V) \geq d$.

(2) If $X = \{i^1, i^2 \ldots i_p\} \in \Gamma_F$, then the two p x m matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots\ldots i_p$ are identical up to a column permutation.

The first condition is called contrast and the second condition is called security.

The collections of matricesC0and C1 are obtained by permuting the columns of the basis matrices S0 and S1 in all possible ways [9].The important parameters of the scheme are

- m, the number of sub pixels in a share. This represents the loss in resolution from the original image to the shared one.

  The m should be as small as possible. The m is computed using the equation:

  $m = 2^{n-1}$ ..... (1)

- α, the relative difference. It determines how well the original image is recognizable. This represents the loss in contrast. The α should be as large as possible. The relative difference α is calculated using the equation:

  $\alpha = | n_b - n_w | / m$ ..... (2)

  Where nb and nw are the number of the black sub pixels which are generated from a black and white pixels in the original image, respectively.

- β, the contrast. The value β is to be as large as possible. The minimum contrast that is required to ensure that the black and white areas will be distinguishable is β≥ 1. The contrast β is computed using the equation:

  $\beta = \alpha.m$ ..... (3)

B. Basic theory

The basic idea of visual cryptography can be best described by considering a 2-out-of-2 VSSS. Let us consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S_1 and S_2, consisting of exactly two pixels for each pixel in the secret image as shown in Table 1. If the pixel in S is black, the dealer randomly chooses one row from the first two rows of Table 1. Similarly, if the pixel in S is white, the dealer randomly chooses one row from the last two rows of Table 1.

TABLE 1. THE PIXEL PATTERN FOR 2-OUT-OF-2 VSSS

Pixel color	Original Pixel	Share1	Share2	Share1+ Share2
Black	■	■□	□■	■
Black	■	□■	■□	■
White	□	■□	■□	■□
White	□	□■	□■	□■

To analyze the security of the 2-out-of-2 VSSS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table 1 for the shares S1 and S2. The pixel selection is random so that the shares S_1 and S_2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. Therefore, this method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared sub pixels. If the superimposition results in two black sub pixels, the original pixel was black; if the superimposition creates one black and one white sub pixel, it indicates that the original pixel was white.

C. Result

Where original secret image(Fig.1a), which is encoded in to two shares: share 1(Fig.1b) and share 2 (Fig.1c).The Fig. 1d is the result of laying share1 over share2 in the '2 out of 2' VSSS scheme.

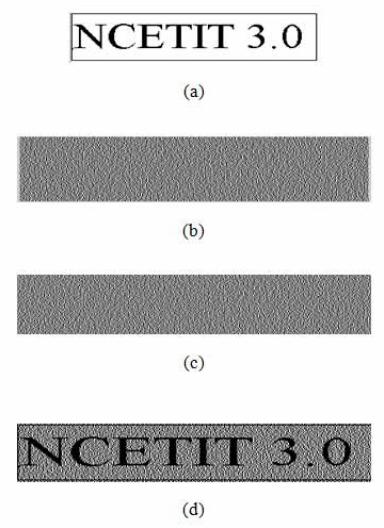

Fig.1. A 2-out of -2 VSSS with 2 sub pixel layout
(a) Original Secret Image ;(b) share1; (c) Share 2;
(d) Retrieved Image (share1 +share2)

The Fig.1 shows 2-out of -2 VSSS with 2 sub pixel layout.

IV. BIOMETRIC TECHNIQUES

Biometric characteristics provide a unique natural signature of a person and it is widely accepted. Each biometric technique has its advantages and disadvantages. The applicability of a specific biometric technique depends heavily on the application domain. No single biometric can meet the entire requirement (e.g. accuracy, cost, practicality, etc.)[14].A brief comparison of biometric techniques based on three factors is provided in Table1.

Biometrics can operate in one of two modes: the identification mode, in which the identity of an unknown user is determined, and the verification mode, in which a claimed identity is either accepted or rejected. On this basis biometrics were applied in many high end applications, with governments, defense and airport security being major customers. However, there are some areas in which biometric applications are moving towards commercial application, namely, network/PC login security, web page security, employee recognition, time and attendance systems, and voting solutions. The biometric systems also enhance user convenience by alleviating the need to design and remember passwords [14].

TABLE 2. COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES

Biometrics	Universality	Performance	Acceptability	Average
Face	100	50	100	83.3
Finger Print	75	100	75	83.3
Gait	75	50	100	75
Hand - Geometry	75	75	75	75
Hand Veins	75	75	75	75
Iris	100	100	50	83.3
Keystrokes	50	50	75	58.3
Retinal Scan	100	100	50	83.3
Signature	50	50	100	66.6
Voice	75	50	100	75

V. ARCHITECTURE OF THE PROPOSED SYSTEM

The systems of our application have following objectives.

- Selection of one of the classical schemes for secret sharing.
- Splitting the secret information [Image] into white and black pixels using selected visual secret sharing scheme.
- Creation of shares with black and white pixels.
- Checking the biometric authenticity of authorized participants.
- Distribution of shares among the participants.
- Stacking the shares to get the secret information.

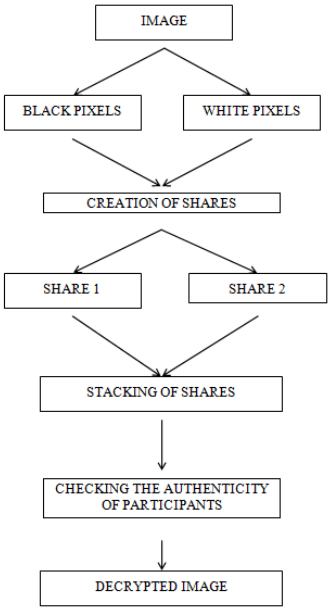

Fig.2 Architecture of the proposed system

VI. CONCLUSION

Even though considerable advancement has been made in security enhancement of visual secret sharing & biometrics over the past decade, the methods have their own drawbacks. By using the visual secret sharing scheme with biometric authentication technique avoids data theft.

This is an overview about the application of secret sharing scheme .The method suggested is widely applicable for information sharing and is more secured .Also it cover the intelligent information management which is now being used in telemedicine.

REFERENCES

[1] Adi Shamir, "How to share a Secret", Communications of the ACM, pp 612-613, 1979.

[2] M. Naor and A. Shamir, "Visual Cryptography",Advances in Cryptology-Eurocrypt '94 *Proceeding, LNCSvol.* 950, Springer-Verlag, 1995, pp. 1-12.

[3] Adhikari Avishek and Bimol Roy."Applications of Partially Balanced Incomplete Block Designs in Developing (2, n) Visual Cryptographic Schemes". *IEICE Trans. Fundamentals,* Vol.E90–A, No.5 May2007

[4] Marek R. Ogiela, Urszula Ogiela, "Linguistic Cryptographic Threshold Schemes",*International Journal of Future Generation Communication and Networking.*Vol.2, No.1,March 2009.

[5] Thomas Monoth, Babu Anto P, "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion".*International Journal of Recent Trends in Engineering,* Vol 1, No 1, May 2009.

[6] N.Radha and S.Karthikeyan, "A study on biometric template security",*ICTACT journal of soft computing,* ,Issue 01, july 2010

[7] S Manimurugan n,K Porkumaran,"A new fast and efficient visual Cryptography Scheme for Medical Images with Forgery Detection". 594 – 599, *ICETECT,* May 2011

[8] Aseel M.Al-Anani,M.H,Abdallah,Randa A.Al-Dallah,Rola I.Al-Khalid, "Multimedia Multilevel Hiding Technique",*European Journal of Scientific Research.*Vol 24,No.1,pp.42-54,2008.

[9] Chi-Chen Chang, Yu-Zheng Wang and Chi-shiang Chan, "An Efficient Probability – based t out of n secret Image sharing scheme". *International Journal of signal processing, Image processing and pattern.*Vol 2, No.1, March 2009.

[10] Chao – Wen Chan and Yi – da Wu, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme". IJCSNS *International Journal of Computer Science and Network Security,* VOL.8 No.4, April 2008.

[11] Levent Ertaul and Vaidehi, "Implementaion of Homomorphic Encryption Schemes for secure Packet Forwording in Mobile Ad Hoc Networks (MANETs)",IJCSNS,VOL.7,No.11,November 2007

[12] Massoud Hadian Dehkordi and Abbas Cheraghi, "Visual Cryptography Schemes with Veto Capabilities". *Australian Journal of BASIC AND Applied Sciences,* 2(4):1239-1245, 2008.

[13] Ren junn Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography".*Tamkang Journal of Science and Engineering.*Vol 3.,No 2,pp 97-106(2000)

[14] Seifedine Kadry,Aziz Barbar, "Design of Secure Mobile Communication using Fingerprint", *European Journal of Scientific Research.*Vol 30,No.1,pp.138-145,2009.

[15] Thomas Monoth & Babu Anto P. "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion", *Proc. ofthe IEEE International Conference on Information Technology* (ICIT '07), (2007), 41-43.