International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

Visual Cryptography Method for Sending Multiple Shares Using Symmetric Encryption Algorithm

B. Divya[1*], D. Sudha[2]

[1]Research Scholar, Department of Computer Science, A.V.C College, Mayiladuthurai, India

[2]Associate Professor, Department of Computer Science, A.V.C College, Mayiladuthurai, India

ABSTRACT

An image can be splitted into two random shares which once individually viewed reveals no idea about the secret picture. The secret image can be obtained by union of the two shares. This method is known as Visual Cryptography. Conventional k out of n visual cryptography scheme *is* used to encrypt a solitary picture into n shares. The image can be decoded by using only k or more shares. Many existing illustration cryptographic methods uses binary images only for this process. This doesn't suits well for many applications. The main objective of this project is to establish message among the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This method eliminates the fundamental safety challenges of VC which is similar to secondary use of code book, random split patterns, expansion of pixels in collective and enhanced images, lossy recovery of secret images and limitation on number of shares. The proposed method is n out of n multi secret sharing method. Broadcast of several secret images at the same time is accomplished through this planned project. The secret picture can be uncovered only when each and every one of the *n* shares are accepted by the receiver and decrypted. Master share is formed at time of encryption by using a secret key and can be regenerated by using the same secret key at the instance of decryption. Experimental results show that the pixel standards of the secret images received at the destination is very elevated *when* compared to the available methodologies.

Keywords : XOR Algorithm, Visual Cryptography, Multi Secret Sharing, Secured Communication, Pixel Expansion

I. INTRODUCTION

Cryptography entails creating written or generated codes that enables know-how to be kept secret. Cryptography converts secret data right into a format with the intention of a beyond the understanding format for an illicit person, allowing it to be transmitted without any person decoding it back into a readable layout, as a consequence compromising the secured data. Knowledge security uses cryptography on a combination of levels. The proficiency can't be learned and a key should be used to decrypt it. The acquaintance maintains the integrity at the course of transit and while being stored. Cryptography additionally aids in non-repudiation. This means both the creator and the beneficiary of the expertise could claim they did not generate or attain it. Cryptography is popularly known as cryptology. Cryptography deals with the respectable achieving of digital data. It refers again to the intend of method founded on mathematical algorithms that afford principal capabilities security

picks. The artwork and science of breaking the cipher textual content is known as cryptanalysis. The cryptographic approach effect will likely be within the cipher textual content material for conversation or storage motive. It entails the purpose of cryptographic method so as to wreck them. Cryptanalysis can be used throughout the design of the novel cryptographic techniques to scan their safety strengths. Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

II. TYPES OF CRYPTOGRAPHY

Text Cryptography

Plain Text

In cryptography, plaintext or clear text is unencrypted information for storage or transmission. Clear text usually refers to data that is transmitted or stored unencrypted.

Cipher Text

In cryptography, cipher text is the result of encryption performed on plaintext using an algorithm. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning cipher text into readable plaintext.

Image Cryptography

Visual Cryptography is a cryptographic manner which makes it possible for photographs to be encrypted in this kind of approach that decryption becomes the job of the character to decrypt by way of sight studying. A visible secret sharing scheme is a method, the place an snapshot was once damaged up into n shares in order that best anybody with all n shares could decrypt the photograph, while any n – 1 shares printed no understanding concerning the original photo. Each share was once printed on a separate transparency, and decryption used to be performed by means of protecting the shares. When all n shares were overlaid, the fashioned picture would show up.

TYPES OF CRYPTOSYSTEMS

Fundamentally, there are two types of cryptosystems based on the manner in which encryption - decryption is carried out in the system:

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the cipher text with the key that is unrelated to the encryption key.

SYMMETRIC KEY ENCRYPTION

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems. A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

The salient features of cryptosystem based on symmetric key encryption are:

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption - decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

ASYMMETRIC KEY ENCRYPTION

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible. Asymmetric Key Encryption are pre-shared secret key between communicating persons.

The salient features of this encryption scheme are as follows:

- Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.
- It requires putting the public key in public repository and the private key as a well guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is strength of this scheme.
- When sender needs to send data to receiver, the public key of receiver is received from repository, encrypts the data and transmits.
- Receiver uses the private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is higher.

SECURITY SERVICES OF CRYPTOGRAPHY

The primary objective of using cryptography is to provide the following four fundamental information security services

Confidentiality

Confidentiality is the most important protection carrier furnished by way of cryptography. It is a protection carrier that maintains the information from an unauthorized man or woman. It is routinely referred to as privacy or secrecy. Confidentiality can be finished through numerous manner commencing from physical securing to the use of mathematical algorithms for information encryption.

Data Integrity

It is safety service that deals with deciding upon any alteration to the information. The data could get modified with the aid of an unauthorized entity intentionally or accidently. Integrity provider confirms that whether or not knowledge is undamaged or no longer since it was once last created,

transmitted or saved via a certified person. Data integrity can not restrict the alteration of knowledge, but presents a way for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. Authentication service has two variants:

- **Message authentication** identifies the originator of the message without any regard router or system that has sent the message.
- **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation

It is a protection carrier that ensures that an entity are not able to refuse the ownership of a prior commitment or an action. It's an assurance that the long-established creator of the info cannot deny the creation or transmission of the mentioned knowledge to a recipient or others. Non-repudiation is a property that is most fascinating in circumstances the place there are possibilities of a dispute over the exchange of knowledge.

The rest of this paper is organized as follows: Section 2 is about the related work about visual cryptography. Section 3 deals with the existing method. Section 4 explains the proposed method. Section 5 is performance evaluation.

III. RELATED WORK

In [1] G. Ateniese et.al., proposes an extended visual cryptography scheme (EVCS), a technique to encode n images, for an access structure (Γ_{Qual}; Γ_{Forb}) on a set of n participants, in such a way that when stack together the transparencies associated to participants in any set X € $\Gamma_{Qual,}$ we get the secret message with no trace of the original images, but any X € Γ_{Forb} has no information on the shared image. Moreover, after the original images are encoded they are still meaningful.(ie) any user will recognize the image on his transparency.

In [2] A. Beimel et.al., shows that any information inequality with four or five variables cannot prove a lower bound of ω (n) on the share size. In addition, it is shown that the same negative result holds for all information inequalities with more than five variables that are known to date.

In [3] M. Bose et.al., employed a Kronecker algebra to obtain necessary and sufficient conditions for the existence of a (k, n) VCS with a prior specification of relative contrasts that quantify the clarity of the recovered image. Also showed how block designs can be used to construct VCS which achieve optimality with respect to the average and minimum relative contrasts but require much smaller pixel expansions than the existing ones.

In [4] O. Farras et.al., proposed the search of bounds on the information ratio of non-perfect secret sharing schemes. This work extends the known connections between polymatroids and perfect secret sharing schemes to the non-perfect case. Proved that there exists a secret sharing scheme for every access function. Uniform access functions, that is, the ones whose values depend only on the number of participants, generalize the threshold access structures.

In [5] M. Sasaki et.al., provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones and also a general method of constructing VSS schemes encrypting multiple secret images.

In [6] S. Washio et.al., examines the security of an audio secret sharing scheme encrypting audio secrets with bounded shares and optimizes the security with respect to the probability distribution used in its encryption.

In [7] Kai-Hui Lee et.al., proposes an algorithm that adopts a novel hybrid encryption approach that includes a VC-based encryption and a camouflaging process. The experimental results demonstrate that the proposed approach not only can increase the capacity efficient for VSSM schemes, but also maintains an excellent level of contrast in the recovered secret images.

In [8] Y. C. Chen et.al., proposes a new notion of non-monotonic visual cryptography (NVC) for human vision system as a primitive to construct FIVC. Presents an ideal construction of simple NVC which relies on a slightly unreasonable assumption. Based on the simple NVC, shows a few methods to extend the functionality for complicated cases of NVC. Then, the generic construction is presented as a systematic manner to eliminate the above assumption. Finally, formally introduce a transformation NVC-to-FIVC algorithm which takes NVC as input and then produce a construction of FIVC. Also, show a demonstration the NVC-to-RIVC algorithm and analyze some properties regarding NVC.

In [9] C.N. Yang et.al., considers the case when the secret image is more than one and this is a so-called multi-secret VCS (MVCS). Also discusses a general (k, n)-MVCS for any k and n. This paper has three main contributions: (1) this scheme is the first general (k, n)-MVCS, which can be applied on any k and n, (2) gives the formal security and contrast conditions of (k, n)-MVCS and (3) theoretically prove that the proposed (k, n)-MVCS satisfies the security and contrast conditions.

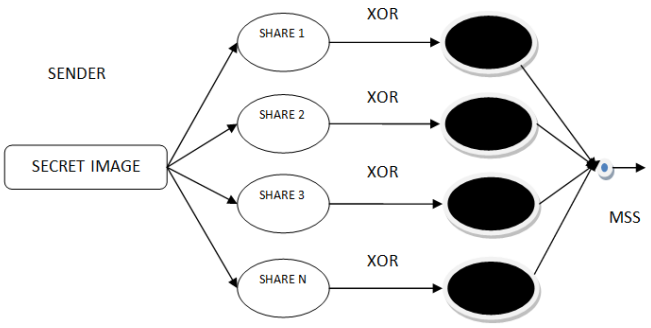
In [10] S. J. Shyu et.al., presents a formal definition to (k, n)-VCS-MS and develops an efficient construction by way of integer linear programming. Experimental results demonstrate the effectiveness of the construction.

IV. EXISTING SYSTEM

In the existing method, the variety of the access control of visual secret sharing (VSS) schemes encrypting a couple of photographs is maximized. First, the formulation of entry structures for a single secret's generalized to that for a couple of secrets. This generalization is maximal in the sense that the generalized system makes no restrictions on access buildings; in unique, it entails the prevailing ones as distinctive circumstances. Subsequent, a ample to be satisfied via the encryption of VSS schemes realizing an entry structure for a couple of secrets of essentially the most general type is offered, and two constructions of VSS schemes with encryption pleasing this are supplied. Every of the two constructions has its expertise in opposition to the opposite; one is extra general and may generate VSS schemes with strictly better distinction and pixel growth than the opposite, while the opposite has an easy implementation. Additionally, for threshold entry buildings, the pixel expansions of VSS schemes generated through the latter building are estimated and become the same as these of the prevailing schemes known as the brink a couple of secret visible cryptographic schemes (MVCS). In the end, the optimality of the previous construction is examined, giving that there exist entry constructions for which it generates no most suitable VSS schemes.

V. PROPOSED SYSTEM

The main objective of this project is to launch secured image transfer between the source and the destination through e - mails and supplementary communicating modes. In this project, users should register with the server to exchange images within themselves. All users should be genuine during the time of registration. An email will be sent to the registered mail. The mail contains a onetime password. The user has to enter it to activate the account. Then only the user is permitted to communicate with other users. An XOR based method using multi secret sharing is implemented to send images from the source to the destination using a secured way. The proposed system eliminates the major safeguard features of VC like exterior use of code book, random share patterns, expansion of pixels in shared and recovered images, lossy recovery of secret images and limitation on number of shares. The proposed method is an n out of n multi secret sharing scheme. Communication of multiple secret shares simultaneously is achieved through this proposed method. The private key will sent to the receiver through mobile. Using that only, the decryption is possible. The secret image can be exposed only when all the n shares are received by the receiver and decrypted. Tentative results show that the pixel values of the secret images received at the destination is very high when compared to the existing methodologies.



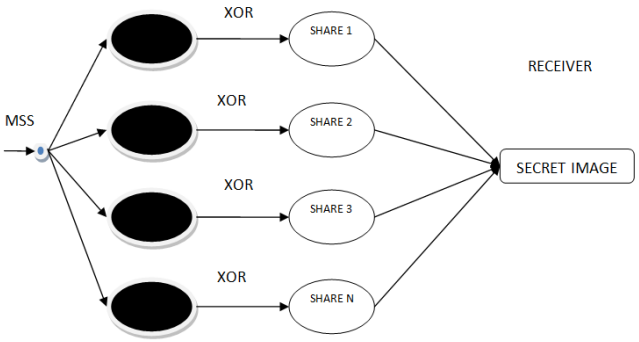


Fig: 1 : System Architecture of the proposed system

VI. PERFORMANCE EVALUATION

To demonstrate the efficiency and feasibility of the proposed XOR based multi-secret sharing scheme, the encrypting/decrypting experiments are conducted on various set images

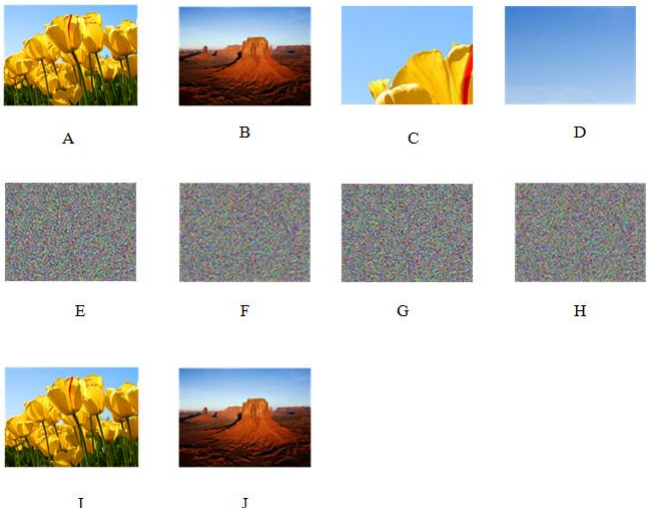


Fig 2 : Experimental Results for n=2 : A- Sen_1, B – Sen_2, C- Sha_1, D – Sha_2, E- Enc_1, F- Enc_2, G – Dec_1, H – Dec_2, I – Rec_1, J – Rec_2

A & B are original images. The original images are splitted using rows and columns. C & D are the first shares of A & B respectively. Like this numerous shares will be formed based on rows and columns. E & F are the encrypted shares of C & D. G & H are the decrypted shares of E & F. I & J are the recovered images. XOR algorithm is used for encryption and decryption.

$$\text{MSE} = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}((I(x,y) - K(x,y))^2$$

MSE is the Mean Square Error value which is for m × n two multi-tone images I and K in which one of the images is original image and another one is share image. From the above examples, it is clear that the size of both the original image and the recovered image are size.

VII. CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. The sender has to select the image that should be sent secretly to the receiver. The secret image is splitted into “n” number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.

VIII. REFERENCES

[1]. G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson (2001) "Extended capabilities for visual cryptography," Theoretical Computer Science, vol. 250, no. 1-2, pp. 143-161.

[2]. A. Beimel and I. Orlov (2011) "Secret sharing and non-shannon information inequalities," IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 5634-5649.

[3]. M. Bose and R. Mukerjee (2010) "Optimal (k, n) visual cryptographic schemes for general k," Designs, Codes and Cryptography, vol. 55, no. 1, pp. 19-35.

[4]. O. Farras, T. Hansen, T. Kaced and C. Padro (2014) "Optimal non-perfect uniform secret sharing schemes," in Proceedings of Advances in Cryptology - Crypto 2014, ser. Lecture Notes in Computer Science, vol. 8617. Springer-Verlag, pp. 217-234.

[5]. M. Sasaki and Y. Watanabe (2014) "Formulation of visual secret sharing schemes encrypting multiple images," in Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014). IEEE, pp. 7391-7395.

[6]. S. Washio and Y. Watanabe (2014) "Security of audio secret sharing scheme encrypting audio secrets with bounded shares," in Proceedings of the 39th IEEE International Conference on Acoustics, Speech & Signal Processing (ICASSP 2014). IEEE, pp. 7396-7400.

[7]. Kai-Hui Lee & Pei -Ling Chiu (2011) "A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images", Optics Communications, June, Volume 284, Issue 12, p. 2730-2741.

[8]. Y. C. Chen (2017) "Fully incrementing visual cryptography from a succinct non - monotonic structure," IEEE Transactions on Information Forensics and Security, May vol. 12, no. 5, pp. 1082-1091.

[9]. C.N. Yang and T.H. Chung (2010) "A general multi-secret visual cryptography scheme," Optics Communications, vol. 283, no. 24, pp. 4949-4962.

[10]. S. J. Shyu (2014) "Threshold visual cryptographic scheme with meaningful shares," IEEE Signal Processing Letters, vol. 21, no. 12, pp. 1521-1525.

[11]. Chen T-H, Wu C-S (2011) Efficient multi-secret image sharing based on Boolean operations. Signal Process 91.1:90-97.

[12]. Taghaddos D, Latif A (2014) Visual cryptography for gray-scale images using bit-level. In: Journal of information hiding and multimedia signal processing, ubiquitous international, vol 5(1), pp 90-98.