SECURE DATA TRANSFER BETWEEN NETWORKS USING FIVC ALGORITHM

Anu Meera.A[1], Malathi. P[2], Sirajnisha.J[3], S.Jenny Kalaiarasi.M.E[4], R.K.Kapila Vani.M.E[5]

UG Student, Department of CSE, Prince Shri Venkateswara Padmavathy Engineering College[1]

UG Student, Department of CSE, Prince Shri Venkateswara Padmavathy Engineering College[2]

UG Student, Department of CSE, Prince Shri Venkateswara Padmavathy Engineering College[3]

Assistant Professor, Department of CSE, Prince Shri Venkateswara Padmavathy Engineering College[4]

Assistant Professor,Department of CSE,Prince Dr.K.Vasudevan College Of Engineering And Technology[5]

ABSTRACT

The sharing of images via visual cryptography is based on encoding and decoding process. In a visual cryptography scheme (VCS), for a set P of n participants, the shares are Xeroxed onto transparencies, and each participant receives one share from a dealer who generates shares from a secret image and distributes them. The main contribution of this concept is to implement the FIVC(Fully Incrementing Visual Cryptography)algorithm. In this the user shares the image into two by sending it as a message and a secure image. The message is converted into image through buffered image technique and then it is generate the visual cryptography image as the secure image is directly generate as a visual cryptography image using FIVC 2 out of 3 algorithm. In this paper, out stating point is to securely share a message using two modes of communication. We split the message key and source based on pixel expansion method.

Keyword: *Visual cryptography, FIVC, sharing of images , pixel expansion method.*

1.INTRODUCTION

Naor and Shamir introduced concept of secret Sharing called VC and other way is called Visual Secret Sharing. In VCS the shares are Xeroxed on to transparencies and each user receives single shares and process them. The users can reconstruct the image by merging the share with or without performing the computation.

The process of VCS includes encoding, distributing, decoding. The process encoding deals with generating shares. The face distributing involve distributing shares to the user. The process decode involves recording the secret image by merging their shares. It shows in fig (1). The past few years the presentation of cheating while sharing multiple secrets become significant. For this purpose they used OR based VC to do secret recovery. Later on, they used binary codes to decode and view the secret image.

The perspective of research methodology, research into the VCSs with meaningful shares can be classified into two techniques: cryptography and embedded techniques. The first approach uses a set of matrices or an algorithm to simultaneously encrypt a VCS and provide a meaningful outlook for the shares of the VCS. The primary method requires designing a set of basis matrices for a specific VCS and suffers from the pixel expansion problem. The main idea behind the RG-based EVCs approach is that it encrypts a secret image to the share according to a given environment specification .The encryption of the secret image can use any of the existing region based VCs. By altering probability p, the algorithm can tune the visual qualities between the recovered image and the shares of an EVCS. The second approach tries to hide shares behind any given message or image covering images.

The user who needs to share the image is split as message and secure image. The message is covered into image using buffered image. The image is generated as a visual cryptography image through FIVC (Fully Incrementing Visual Cryptography)2 out of 3 algorithm. The secure image is directly generated as a visual cryptography image. The visual cryptography image is split into two images namely, key image and source image .While splitting key image it is done based on the pixel part input image where as the source image splits based on the combine input image and key image. The key image is send to the receiver's mail. The source image is send to the receiver by obtaining the receiver's IP. To view the original image which is received should be combined. The original data (image) is viewed based on the 2 out of 3 visual cryptography.

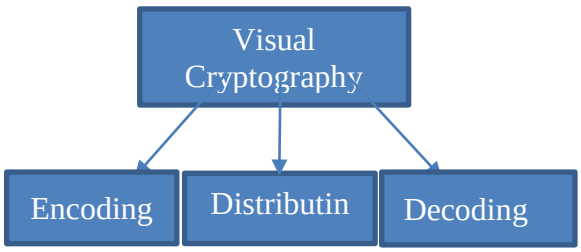


Fig (1):Process of Visual Cryptography

Related Work

a.Visual Cryptography

Visual Cryptography (VC) is a technique that encrypts a Secret image into n shares, with each participants holding one share, any participant with less than k, $2 \leq k \leq n$ Shares cannot give any information about the secret image. Stacking the k shares opens up the secret image, which can be recognized by the human visual system. Conventional shares, consist of many random and meaningless pixels satisfies the security purpose for protecting secret contents, but the drawback in it is a high transmission risk because of noise-like shares which raise the suspicion of attackers, who may hack the shares. A 2-out-of-n binocular VCS, called the (2, n)-BVCS, is proposed to provide non-altered high quality cover images for shares of the VCS to decrease the risk of hacking during the transmission. The proposed (2, n)-BVCS shares a binary code image with n participants when any two participants stack their transparencies, The encrypted secret is revealed only when the code is known.

b. The Two-Phase Encryption Procedure

In this study, we propose a (2, n)-BVCS for sharing a binary Secret image in n SIRDSS. The proposed two-phase encryption process is shown in fig.3.In the first phase ,n depth maps are used to produce n SIRDSS using the auto stereogram generator that adopts thirmbleby's algorithm. In the proposed (2, n)- BVCS, each depth map has the same image size and all Generated SIRDSS have the same pixel density d. In the second phase, according to construction rules for (2, n)-BVCS, pixels in the n generated SIRDD are altered to share a binary secret image for the SIRDSS by the (2, n)-BVCS encryptor.

2. EXISTING SYSTEM

The Existing System, once the input message is given, it is then split into source part and key part. The one part of the grid is taken by the key image. The another part of the grid is taken by the source image. The image is directly send to the server. Then the source image already in a server. In between the hacker hack the key image .Then he would check the matches the image is found or not. They frequently map key with any other source image. Once the image is found the hacker easily hack the original image.

TECHNIQUES

RIVC:

It is defined as a Region Incrementing Visual Cryptography .The input image considered as a whole with in a part of grid is taken as a key. So it is based on region incrementing visual cryptography.

Algorithm:

In existing system using a RG-based-EVCS (Extend Visual Cryptography Scheme).It is based on using quality of the image.

Disadvantages:

1. Less Security.

2. Slow and more expansive to tabulate.
3. Time Complexity.

Fig (a): Input Image

Fig (b): Key Image

3.PROPOSED SYSTEM

In Proposed system we are using a Visual Cryptography. The input can be a text format and image format. Once the input message taken, it will be converted in the form of buffered image using buffered image method in java. Then this buffered image generate a Stereogram image i.e a Random dot stereogram. The Stereogram image is split in to two parts one is key image and another one is source image based on FIVC 2 out of 3 algorithm. The key image is depend on the original image with pixels of binary codes. The source is depend on the original image and the key image. The key image is send to the receiver's mail id. Then the source image send to receiver's system IP address. Finally, receiver got the two images, combine those images, and view the original image.

TECHNIQUES

Non Monotone :

It is defined as independent shares of images. Once splitting the input images there is an independent of shares. So no one can hack the image.

Algorithm:

FIVC :

It is a Fully Incrementing Visual Cryptography. The full part of input image is split as an equal share based on pixel expansion method.

Advantages:

A. Sharing secret information with high security using Random dot stereogram images.
B. Cannot decrypt the image from inside to outside hacker.
C. Hacker cannot hack the both modes of communication.
D. Only to the authorized user the file is sent and viewed.

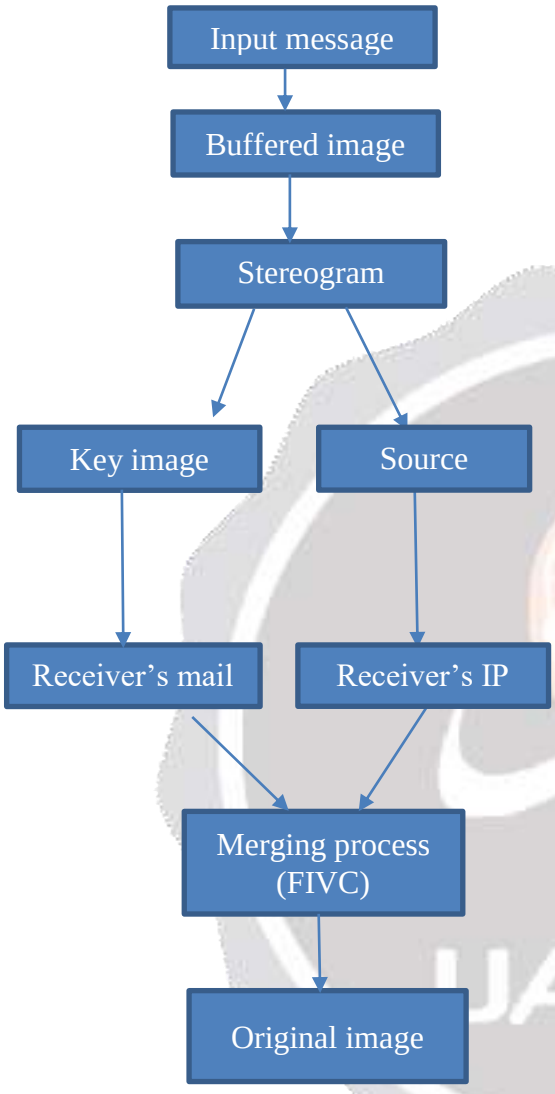


Fig (2) : Process of message from source to destination

4. IMPLEMENTATION

A. Input Image Creation :

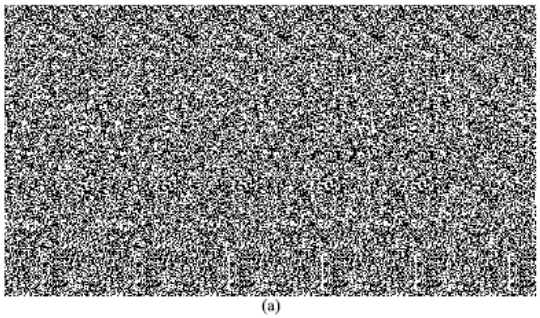
In visual Cryptography , the image is shared securely from the sender to receiver. The sender distinguish the image into message and secure image. The image is converted into buffered image and generates a visual cryptography.

Hay How Are You

Fig: Example of Buffered Image

Convert Stereogram Image :

The converted image is defined as stereogram image which is generated as visual cryptography image using FIVC 2 out of 3 algorithm



(a)

Fig: Example of stereogram image

B. Split Image process :

The Visual Cryptography concept generate VC image which is split into two types of images namely key image and source image. Key image is based on single pixel part of the input and other part is source image. Source image is based on both key and source image.

Fig :Splitting images

C. Transfer of images :

The image that is split transferred to receiver into two ways. The key image is obtained by the pixel part of input images is send to the receiver through g-mail API. The source image is stored in server and it is send to receiver by obtaining the receiver IP address.

D. Merge Images:

The images which is send to the receiver into two different methods. To view the original data the receiver should use the 2 out of 3 technique. In this process, the key and source image combine to the both and view the original image . The merging of images should display the original data.

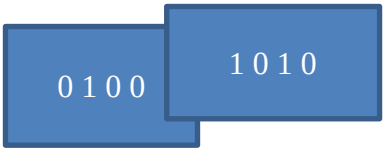
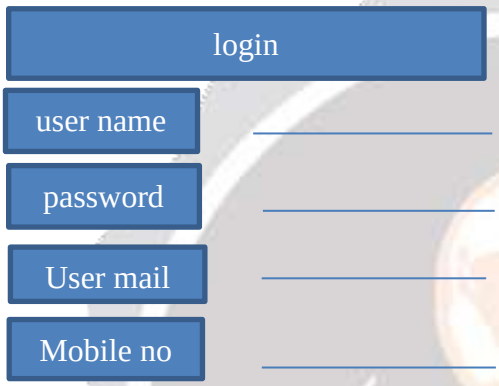


Fig: Merging key and source image

E. User Profile Update

In this module use of the modify and update the user details. The new user will be register this application it used to send or share visual secret information's. This module used to send or share the visual secret information's. This module used to update user information and contain following sub modules are login and registration. Then this module used to contact the user with in some groups.



4.FUTURE ENHANCEMENT

Now we are using a two shares of input image. In future we are making three shares. Those shares send to independently. So compared this three shares with two shares which is more security . Then applying a OTP generation in viewing of image , it is also more secure no one can hack the original image.

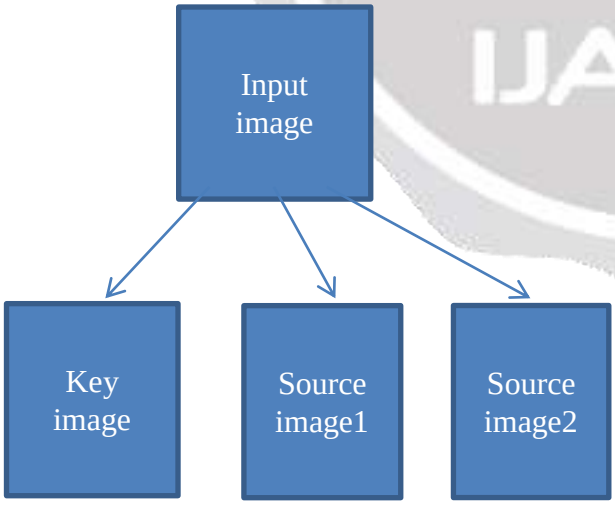


Fig: Splitting of three parts

6. CONCLUSION

A Modular method to construct FIVC from the proposed primitive, NVCS. It rely on an assumption and used traditional VC to construct the atomic method for NVCS, and then show some extensions including widening, multi-atomic, and full-fledged methods. A generic construction is presented to eliminate the assumption. The throwing

redundancy technique is proposed as a tool to decrease the pixel expansion. The notion of NVCS can potentially find other application or purposes and is of independent interest.

7. REFERENCES

[1] G.Ateniese. C. Blundo. A. De Santis. D.R. Stinson. Visual Cryptography for general access structures. Inform. And Comput,129(2)(1996)86-106

[2]Carlo Blundo. Alfredo De Santis. Moni Naor. Visual Cryptography for grey level images. Information Processing Letters.75(2000)255-259

[3]A. Thomas Hofmeister. B. Matthias Krause. Hans U. Simon.A. Contrast-Optimal k out of n Secret sharing schemes in visual cryptography. Theoretical Computer Science 240(2000)471-485

[4]N. Linial. N. Nisan, Approximate inclusion –Combinatorial 10(1990)349-345

[5]S.Droste, New results on visual cryptograpy,in:"Advances in Cryptography"-CRYPTO'96,Springer,Berlin,1996, pp. 1-12.

[6]P.V.Chavan and RS Mangrulkuar,"Encrypting information color image using color visual cryptography,"3rd IEEE International Conference,vol. 2,pp.277-281,2010.

[7]Ching-Nung Yang, Senior Member, IEEE, and Dao-Shun Wang, Member, IEEE. Circuits and systems for video technology,vol,24,No.2,Feb 2014.

[8]Giuseppe Ateniese, Carlo Blundo and Alfred De Santis, Douglas R.Stinson. Information and computation 129,86-106(1996).

[9]Shyong Jian Shyu and Ming Chiang Chen. Information forensics and security,vol.6.No.3.sep 2011

[10]G.K Blakley , "Safeguarding cryptographic keys."proc. National comput. Conf.,1979.vol.48.pp.313-317.