International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 1

Visual Cryptography for Image Processing: A Survey

Soundarya B A, Sowmeya D, Yazhini G V
Department of Information Technology, Sri Krishna College of Engineering and Technology
(An Autonomous Institution Affiliated to Anna University, Chennai.), Coimbatore, Tamil Nadu, India

ABSTRACT

The method in which the visual information is encrypted by the process of encryption and those encrypted images are decrypted via sight reading is said to be called as visual cryptography or it is a method to hide the picture or an image into non-identical number of shares (different shares) and they are distributed to different set of participants. There are two sets of participants namely qualified and unqualified. The qualified set will combine with the participants of non-qualified set in order to get the secret image. Or the qualified set of participants alone can get the secret image. This new system has two phases. In the initial phase, the secret image as an input generates or creates some meaningless shares (4 shares) based on an algorithm called GAS algorithm. In next phase, the cover images are added in each share. They are added using an algorithm called stamping algorithm and distributes the embedded pictures or images to the participants. In receiver end, the embedded images are processed to receive the covering images from the shares generated and by overlapping those shares, the secret images are retrieved. These shares are arranged in correct order. In proposed system the security problem and the pixel expansion problems are reduced. It also helps to increase in the number of shares. Finally the obtained secret image can be viewed in a high resolution.

Keywords: *GAS Algorithm, Stamping Algorithm, Pixel Expansion, Shares.*

I. INTRODUCTION

Nowadays, transferring of files and sharing the information via internet have been increased rapidly. Therefore, there is a threat from the many hackers, unauthorised users and the third party users. They can easily access the secret information by hacking. This is one of the major problems faced by the many users who shares information via internet. The fast growth in the technology and advancement provides easy and convenient sharing or transferring of data over internet. Much confidential data like military information, signatures and images are sent. While sending secret documents like images, text over the network, security issue occurs. This issue is due to the poor link in the public network. Since there is a high chance of stealing the secret information by the hackers, we are in need of a proper algorithm in order to deal with these security issues of secret images. So Visual Cryptography helps in secure way of sharing the information over the internet.

Visual cryptography for image hiding was initially invented in 1995 by "Moni Naor and Adi Shamir" [1]. It is a method in which the images are shared to some set of qualified participants by the process of encryption. So that these encrypted images is decrypted to get the secret information by human vision. The secret information is received by entering the correct key. These keys are used in two phase namely initial and final phase (sender and receiver). Here, the images are split into shares for transmission. Each and every share is considered as an individual image. The first image contains some randomly shuffled pixels and the other image has the secret information. It is an

impossible event to receive the secret information without joining or overlapping the images which was shared. Using this specific technique, the image is encrypted. So that no third party users apart from the users of sender side and receiver phase. These users can only get the original image. This feature provides high security. This technique is used in applications like areas of biometric security and watermarking. It is also used in remote electronic voting and customer identification in banking.

II. LITERATURE REVIEW

In this section the various surveys about the Visual Cryptography for Image Processing has been clearly explained.

In the paper proposed by the authors "M. Naor and A. Shamir", the problems like encrypting the written material such as printed text files, hand written notes and pictures are reduced. They are perfectly shared in a secure way in which it is decoded directly or indirectly by the human vision. The primary model has a page printed by ciphertext which is faxed or sent by mail. This printed transparency acts as a secret key. The first text (original clear text) text is revealed or exposed by keeping the printed transparency with a key on that page with the ciphertext. . This system is somewhat similar to OTP method (one time pad). i.e each page decrypts the cipertext with various transparency. Because of this simple method, many unauthorized users can use the system without knowing any knowledge about cryptography [1].

In the paper proposed by the "M. Naor and B. Pinkas", the methods like visually identifying (visual identification) and authenticating (authentication) data are explained [2]. These methods are convenient to use and it can be implemented by simple and common “low tech” technology. The major advantages of this system are the physical requirements. They are linear in nature in their message size and logarithmic in the fault probability p. Each and every scheme defines on the specific capabilities where the qualified participants should maintain the scheme to be in a secure way. In some of the cases the specific capabilities are quantified and the measure of complexity is connected to the quantification parameters. Those assumptions about human capabilities are verified through various experiments and the protocol is proved to be safe and secure. The major drawback explains about the visual authentication methods that are applicable for any kind of visual data such as numerical and textual data or graphical data. These methods are used only for one time or single authentication [2].

In the paper proposed by authors "A. De Bonis and C. Blundo along with A. De Santis " have analyse the cryptography scheme in reconstruction of the black coloured pixels is absolute and perfect which means all the sub-pixels seen within the black pixel are seen to be black. For any value of k and n, where $2 \leq k \leq n$, we give a construction for (k,n)-threshold VCS which improves on the best previously known constructions with respect to the expansion of the pixel. they also provide a construction for coloured (2,n)-threshold VCS and for coloured (n,n)-threshold VCS. Both the constructions helps in better improvement over the previously known constructions which is respect to the expansion of the pixel. [3].

In the paper proposed by authors, "G. R. Arce, Z. Zhou, and G. Di Crescenzo", a novel method called halftone technique in visual cryptography is explained. This is suggested to achieve the visual cryptography by halftoning method. A principle called blue-noise dithering, uses an algorithm called "void and cluster algorithm" in the newly proposed system. This algorithm encodes a single image (binary secret image) into much number of shares (n halftone images) which carries important visual information. This process shows that the obtained halftone share's visual quality is far better than any other methods in visual cryptography. [4].

This paper was proposed by the authors "Arce G. R and Di Crescenzo. G along with Z. M. Wang." They describes that the cryptography scheme (VCS) will produce or generate more number of shares (n shares) with reduced image size that are transparent and supports different variety of image formats. It also presents an integrated approach for binary images, Gray scale images and coloured images by maintaining the pixel expansion and visual quality with more resolution. [5].

In the paper proposed by authors "D. S. Tsai, T. Chenc, and G. Horng", a simple method for transforming meaningless shares into VSSS to normal colourful images is explained. The final output of this experiment shows that this method gives a basic answer to the k-out-of-n VSSS with some additional pixel expansions and low power computation when compared to other methods. [6].

III. RESEARCH METHODOLOGIES

The diagram of design architecture briefly justifies the overall flow in the system. It describes the main process and flow of the module. First of all, it generates the needed shares, followed by the process of embedding the images and at last extraction process takes place for the images that are generated. The remaining process takes place inside the blocks. Generally, there are three important processes which are implemented in this new system. At the starting phase (i.e. Sender side), the previously processed picture (an image) is encrypted by use of an algorithm called as "GAS algorithm". This image is protected by password authentication. It is to prevent the unauthorised accessing of data from the third party users and it also helps to avoid the security issues. The image is split into more shares by share synthesizer. These shares are distributed to the qualified participants. In next embedding phase, these shares are stamped with one another shares using the covering images. Now the embedded images are ready to send to the users in the receiver end. At the extraction end, the shares are extracted by overlapping the covering images and shares are arranged in appropriate order to get accurate data. Finally with the help of password verification, the information is shared secretly. There are three modules namely:

- Generation of Share
- The Embedding Process
- Recovering Images

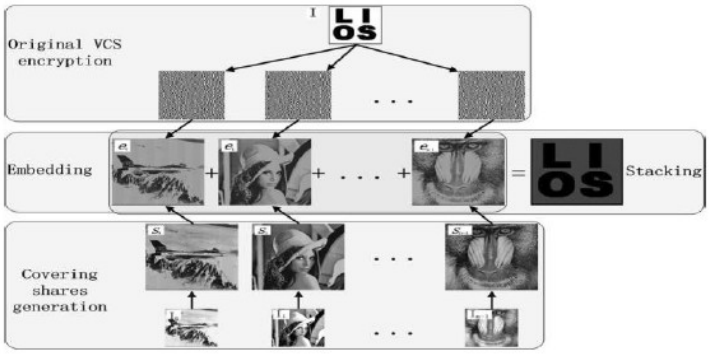

Figure 1: Overall Module Diagram

GENERATION OF SHARES

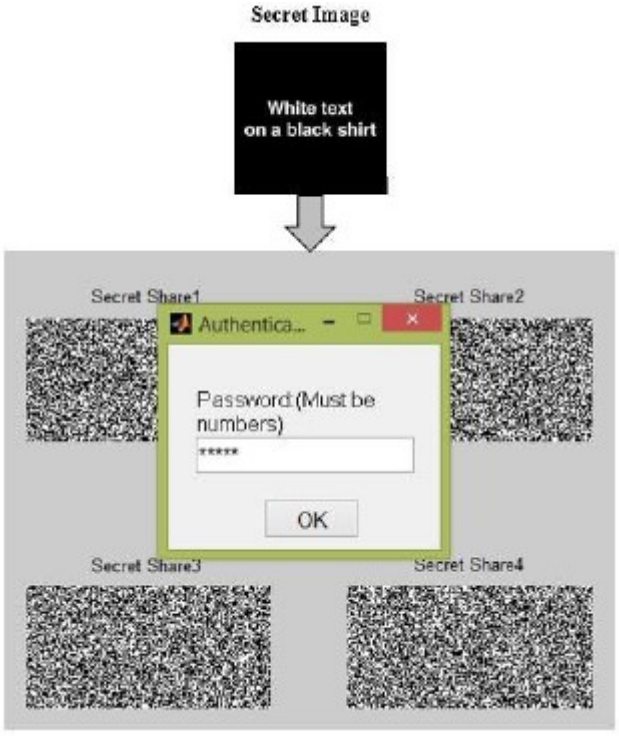

Figure 2: Generating the Shares with Authentication

THE EMBEDDED PROCESS:

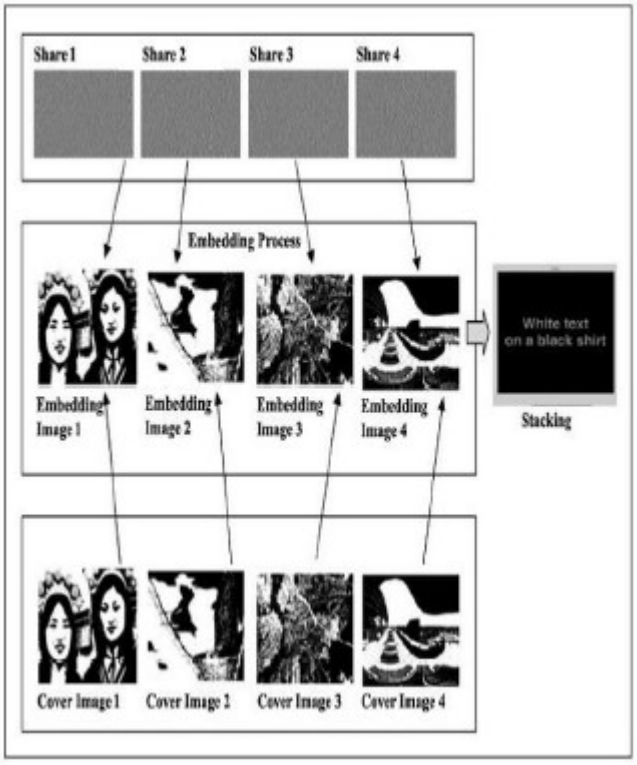

Figure 3: Embedding Process

EXTRACTING PROCESS:

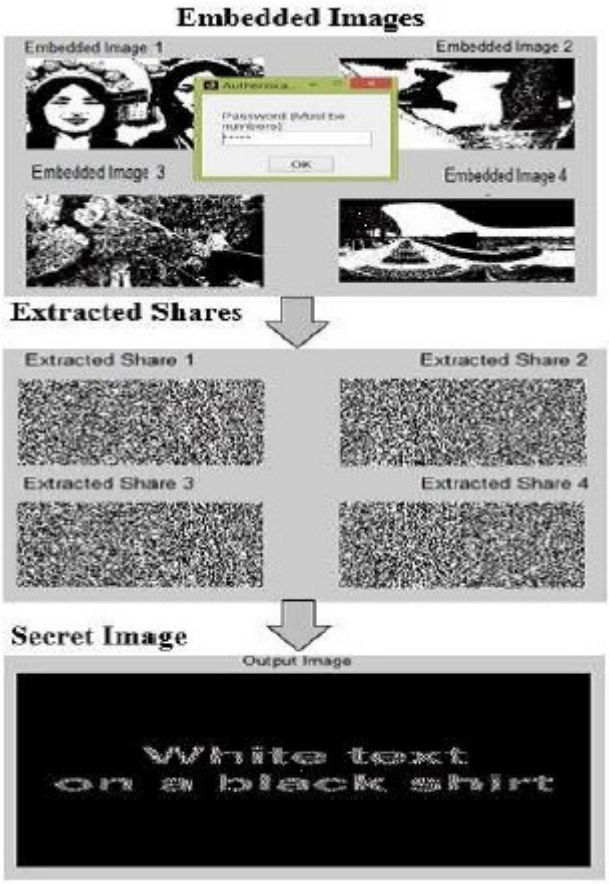

Figure 4: Extraction Process

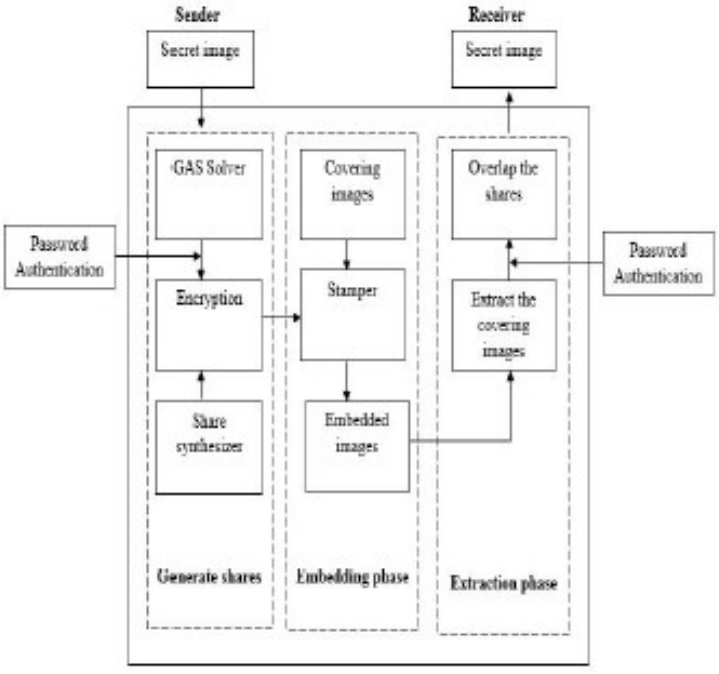

Figure: 5 Architecture Diagram of the Proposed System

IV.CONCLUSIONS AND FUTURE WORK

An encryption method that uses the GAS (General Access Structures) algorithm is known as Visual Cryptography Scheme (VCS). The problem of pixel expansion is totally reduced by commonly increasing the share quantity. this also makes good and high image resolution with better image quality. A scheme in which sharing the information anonymously (secretly) between the users is called as secret sharing scheme. This is a different method for a group of individuals or participants to share the secret information. Depending upon the number of individuals, the share synthesizer will split the image. To make the image even more protective, the divided shares are embedded among one another with covering images by an algorithm called stamping algorithm. At the final end (receiver side), the secret image is obtained by stacking or overlapping the shares in the perfect order. The password verification or authentication on both sides keeps the system more secure. It is an impossible task for the hackers to find the secret image because the images are covered by using meaningless shares. The quality of the image and the size of the image is measured by EVCS and GAS algorithm.

The future work requires, even more increasing in number of shares for better image quality and to implement the secret colour images by sharing the multiple secret images using various methods.

V.DISCUSSION

The existing EVCS is compared with the newly proposed GAS solver algorithm. The values related to the images are noted and tabulated which describes the memory size of an image and all the dimensions of an image. The five secret images are studied and analysed in this section. In EVCS method, the two shares divided and stacked to receive the original private image (secret image). But by using the GAS solver algorithm, the secret image is split up into four number of shares which is retrieved with high resolution. The graph shows the variance in between the EVCS and GAS algorithm. Higher the memory size leads to high resolution. The most important property of visual cryptography is that, the decryption of the secret images requires neither the knowledge of cryptography nor complex computation.

REFERENCES

1) M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT‟ 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.
2) M. Naor and B. Pinkas, “Visual authentication and identification,” Springer-Verlag LNCS, vol. 1294, pp. 322–336, 1997.
3) C. Blundo, A. De Bonis, and A. De Santis, “Improved schemes for visual cryptography,” Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.
4) Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
5) Z. M. Wang, G. R. Arce, and G.Di Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009.
6) D. S. Tsai, T. Chenc, and G. Horng, “On generating meaningful shares in visual secret sharing scheme," Imag. Sci. J., vol. 56, pp. 49-55, 2008.
7) M.Amarnath Reddy, P.Shanthi Bala, G.Aghila, “Comparison of Visual Cryptographic Schemes,” IJEST, vol. 3 no. 5, pp. 4145-4150, 2011.