Bit Slicng based Visual Cryptography On Gray Scale Image

K.Sindhu
Student, Computer Science Department
UCEK, Kakinada
Andhra Pradesh, India
e-mail:sindhukallam@gmail.com

Ch.RatnaKumari
Asst Prof, Computer science department
UCEK, Kakinada
Andhra Pradesh, India
e-mail:ratnamala3784@gmail.com

K.Srinivasa Rao
Asst Prof, MCA department
Yogi Vemana University, kadapa
Andhra Pradesh, India
e-mail:kanususrinivas@gmail.com

***Abstract*—** Data transmission through online is become mandatory in recent ages. No one can avoid data transmission over internet. But sensitivity of the data to be considered while transmits over internet. Internet is public medium where everyone has equal right to do their activities. Like in general public, internet also having malicious users and their main activity is deployment of attack. These attacks are of many types such as hacking, tampering and eavesdropping etc. Efficient data hiding techniques are required to with stand these attacks or to escape from these attacks. Visual Cryptography is one of such techniques to hide multimedia data in other multimedia data such as images, audio files or video files. In the proposed system secret image is partitioned or divided into shares based on the bits. These shares are then covered with given cover images then these covered shares are distributed to 'n' participants. To recover the secret all those participants are required. The proposed approach followed a novel method of bit slicing on gray scale images. So at the time of recover secret image cant' be visible with same intensity or resolution as that of original image. For this purpose four secret keys are used. Simulation results shows that when compared to existing schemes , proposed approach can hide the image under cover images in efficient way as well as recovering of secret also lightweight and resilience to attacks.

Keywords: *Visual cryptography, bit slicing, lightweight cryptography, resilience*

*****

I. INTRODUCTION

Visual Cryptography is another technique for achieving data security [1]. It is a cryptographic method in which cipher text can be decoded directly by the human visual system. Decryption process does not require any computational device, and it is a mechanical operation. Thus, it eliminates the drawback of hardware and software requirement, which is needed for the decryption process in traditional cryptography. In Visual Cryptography [1], one secret image is encoded into n shares and each share is given to one of the participant in the group.

Each participant cannot decrypt any information from his own transparency, but when at least k of them superimpose their shares pixel by pixel, they retrieve the secret from the superimposed result by using their visual system. Such a scheme is called (k, n) visual secret sharing VSS" by E.R verhaul and H.C.A.V.Tilborg [3]. Any k shares can be stacked to retrieve secret. By Stacking of k − 1 or less does not reveal the secret. When k or more transparencies are superimposed, is proportional to the number of superimposed transparencies. So that the decryption process requires only human visual system instead of any computational device. It is much useful in situations where computing devices are not available [2].

Visual cryptography which allows the encryption of secret information in the image form.Visual secret sharing scheme is which a image was broken up to n shares could decrypt the image by stacking all the transparencies together. Extended visual cryptography which adds a meaningful cover image to each share. Someone with all n shares could decrypt the image the decryption becomes a mechanical operation.

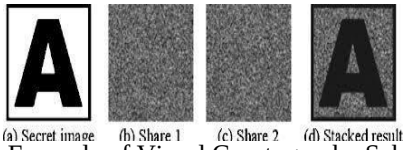

Fig 1 Example of Visual Cryptography Scheme

II. RELATED WORK

In the year 1994, Naor and Shamir [1] introduced the concept of visual cryptography to encode a binary image into two shares, share1 and share2.The decryption can be performed by using human Visual System (HVS).kai-Hui Lee and pei-Ling chiu [2] proposed a two phased encryption algorithm. In the first phase based on the access structure construct shares using some optimization technique. In the second phase add a cover image to each share by using stamping algorithm. E.R.Verhaul and H.C.A.V.Tilborg [3] introduced k out of n visual cryptographic scheme. This is an extension to Naor and Shamir model. In the past decade, many research results on the threshold visual secret sharing scheme (also known as k-out-of-n VSS scheme or (k-n)VSS scheme) have been proposed [2]–[9]. G.Ateniese,C.Blundo,A.D.Santis [10] proposed the concept of general access structure (GAS) and also developed a VC-based solution for some GASs .Afterward, Hsu proposed the unexpanded VCS for a GAS problem as an optimization model [11], [12]. F.Liu C.wu and X.Lin proposed a step construction of visual cryptography [13]. For example there are four participants—one CEO, one manager, and two employees—sharing a secret image, the CEO may decrypt the secret with any one colleague who holds one of the other shares. The manager is allowed to get the secret with only two employees. The two employees are restricted access to the secret. Due to these flexibilities, dealers can also set the number of shares as the decrypting condition. Hence, the –

VSS scheme can be known as a special case of the GAS. Conventional VSS schemes delivered noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem. Hence, researchers have developed the extended visual cryptography scheme (EVCS [14], also known as the friendly VC scheme [15], [16]), which adds a meaningful cover image on each share to address the management problem. Ateniese presented a general technique to implement -threshold EVCS as well as various interesting classes of access structures for binary secret images [14]. Fang [15] and C.Blundo A.D.Santis [16] proposed VC-based and random-grid-based techniques, respectively, for –EVCS with a progressive decryption effect. Wang *et al.* developed a matrix extension algorithm for -EVCS by modifying an existing VCS with random-looking shares, which were then utilized as meaningful shares [17].J.Weirand W.yan [18] proposed a plane transformation visual cryptography. The pixel expansion problem is a disadvantage with most of the VSS schemes. The contrast of the recovered images will be decreased to simultaneously. The pixel expansion problem not only affects the practicability of storage/transmission requirements for shares but also decreases the contrast of the recovered secret images [19]. so, the existing EVCS algorithms for GASs cannot avoid the pixel expansion problem[20]. Therefore, to find a solution to this problem proposed a novel technique called bit slicing for division of shares.

III. Existing System

Extended visual cryptography scheme for general access structures address the pixel expansion problem. The pixel expansion problem means it effect the storage /transmission needs of shares and it degrades the contrast of the recovered image. In the existing System they use GAS solver technique for division of shares which needs complex mathematical optimization techniques.

IV. Proposed System

This section consists of proposed architecture to the existing system. In the proposed system secret image is partitioned or divided into shares based on the bits. These shares are then covered with given cover images then these covered shares are distributed to 'n' participants. To recover the secret all those participants are required. The proposed approach followed a novel method of bit slicing on gray scale images. So at the time of recover secret image cant' be visible with same intensity or resolution as that of original image. For this purpose four secret keys are used. Proposed visual cryptography procedure is described as follows.

It takes either RGB or gray scale image as input. If given input is RGB image then it is converted into gray image. Given secret image is converted into bit slices and placed in the shares. At least two and at most eight shares are required to apply proposed approach. Here we considered three shares.

Each pixel of gray scale image contains 0-255 contrast levels. Any number of this range can fit in 1Byte of memory can be represented with 8 bits. By taking this analysis as a basis 1, 4, 7 bits of each pixel value is store in the first share, 2, 5, 8 bits of each pixel value is stored in the second share and balance bit positions 3 and 6 are placed in the third share. Initially these shares contain zero values. After this bit distribution they are replaced with equivalent gray values.

Now these shares have to be hiding in the cover images. For this purpose n cover images are required. To hide the i^{th} secret share in the i^{th} cover image four secret keys are chosen. Among those four keys are two are divisors and two are excepted remainders. To hide the i^{th} secret share in the i^{th} cover image the modulus of cover image and secret image should be equal by dividing them with same divisor final shares contain those pixel of secret image whose intensity levels should match with cover image due to that, matched gray level can generate same remainder.

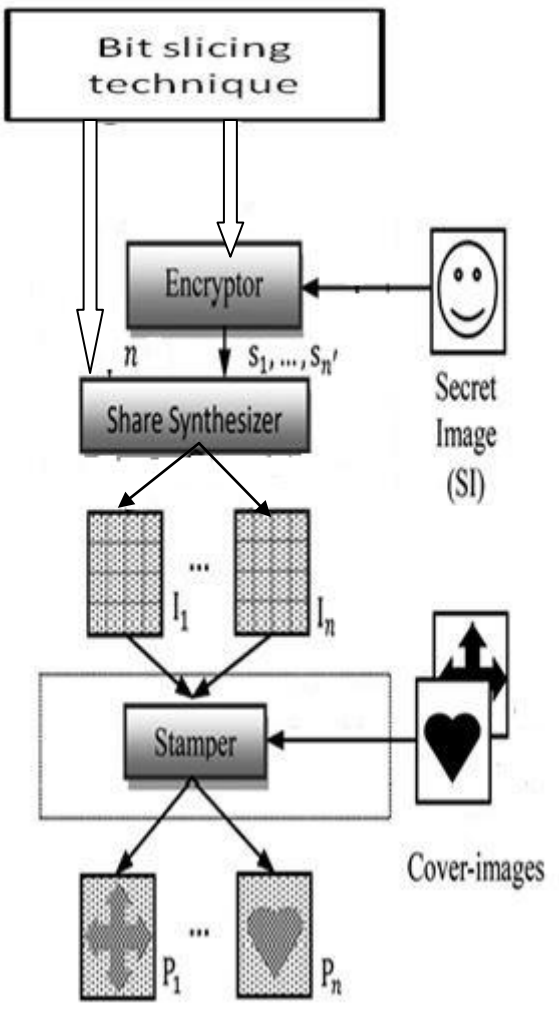

Fig 2 Solution procedure for gray scale images.

To keep track of those positions in all the secret shares three sparse matrices are generated. They are used to recover the images by verifying the same pixel positions. The four keys can be distributed or maintained centrally by any trusted third party for recovery of image. But if we want to distribute those four keys they should be jumbled. Here care should be taken while choosing divisors and remainders in such a way so that cover images should not be affected or destroyed in full length.

Next process is reconstruction or recovery of secret from the distributed covered shares. Reverse process is

 ISSN: 2321-8169
2317 – 2320

required to get the secret. For that tracked and stored sparse matrices are used along with secret keys. Choose those pixel positions respectively from the sparse matrices and divide with same divisor and compare with the same remainder while encrypting. Result of this process generates merged version of n shares. Now apply color map on the merged version to differentiate the gray intensity levels. Recovered secret look like a shadow or outlined image of original secret image.

Proposed approach uses visual cryptography on gray scale images with bit slicing technique. Observe that bit slicing is not applied or reversed at the time of secret recovery. So final recovered secret may not necessarily displayed as original secret. This shows that computation using all the four secret keys and bit slice is lightweight and resilience to stenography attacks.

V. SAMPLE RESULTS

Fig 3 Input Secret image

Fig 4 Share 1 of Bit Slicing

Fig 5 Share 2 of Bit Slicing

Fig 6 Share 3 of bit Slicing

Fig 7 Cover image 1 Contains Share 1

Fig 8 Cover image 2 contains share2

Fig 9 cover image 3 contains share 3

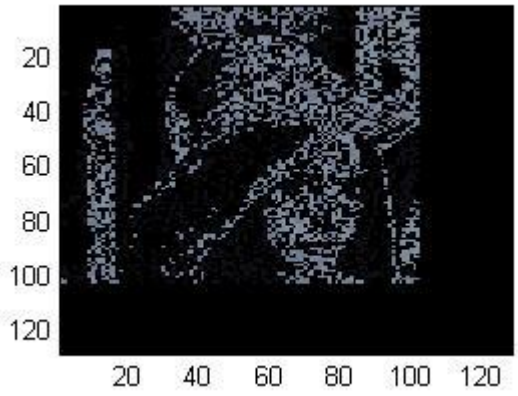

Fig 10 Recovered Secret image

VI. CONCLUSION

Hence, proposed approach followed a novel method of bit slicing on gray scale images. So at the time of recover

 ISSN: 2321-8169
2317 – 2320

secret image cant' be visible with same intensity or resolution as that of original image. For this purpose four secret keys are used. Simulation results shows that when compared to existing schemes , proposed approach can hide the image under cover images in efficient way as well as recovering of secret also lightweight and resilience to attacks.

Future extension to proposed approach will be applying of bit slicing and visual cryptography on RGB images

References

[1] M.Naor and A.Shamir, "Visual CRYPTOGRAPHY" in Cryptology(Eurpocrypt'94), 1994, pp.1-12.

[2] Kai-Hui Lee and Pei-Ling Chiu"An Extended visual Cryptography for general access structures", vol. 7., No 7, Feb 2012

[3] E. R. verheul and H.C.A.v.Tilborg, "Constructions and properties of k-out-of-n visual secret sharing schemes" Designs Codes Crypto, , vol. 11, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 179–196, 1997

[4] A.Shamir"how to share a seret, "communications vol 22, pp612-613

[5] A.Adhikari and S.Sikdar, "A new (2, n)-visual threshold scheme for color images, " in Proc INDOCRYPT 2003, Berlin, Germany., pp.148-161..

[6] C.Blundo, P, D'Arco, A.D.Santis, and D.R.Stinson, , "Contrst Optimal threshold visual cryptography schemes, " IEEE Transl. J. Magn. Japan, vol. 16, pp. 224–261, 2003

[7] C.N.Yang, "New Visual secret sharing schemes using problabilistic method" pattern Recongnit lett, vol 25, pp.481-494, 2004

[8] C.Blundo, S.Climato and A.D.Santis"visual cryptographic schems with optimal pixel expnsion", theor comput, sci, vol 369, pp.169-182, 2006.

[9] P.L.Chiu and K.H.Lee"A simulated annaling algoritham for general threshold visual cryptography schemes" IEEE trans.inf.Forenics security, vol 6 pp. 992-1001, sep 2011.

[10] G.Ateniese, C.Blundo, A.D.Santis and D.R.Stinson, . , "visual cryptography for general access structures, " inform comput, vol 129, pp.86-106, 1996.

[11] C.S.Hsu and Y.C.Hou, "Goal programming assisted visual unexpanded shadow images for general access structures"opt Eng., vol 45, no 9, 2006.

[12] C.S.Hsu, S.F.Tu and Y.C.Hou, "An optimization model for visual cryptography schemes with un expandd shares , "Found Intelligent Syst.LNaI, vol .4203, pp.58-67, 2006.

[13] F.Liu, C.Wu and X.Lin, "Step Construction of visual cryptography schemes"IEEE trans .inf.Forencics security, vol 5, pp 27-38, Mar 2010.

[14] G.Ateniese , C.Blundo , A.D.Santis and D.R.Stinso.n, "Extended capabilities for visual cryptography, "vol 250 pp 143-161, 2001.

[15] W.P.Fang , "Friendly Progressive visul secret sharing, "pattern Recognit, vol 41, pp 1410-1414, Apr 2008.

[16] C.Blundo and A.D.Santis, "visual cryptography schemes with perfect reconstruction of black pixels"vol 22, pp 449-455.

[17] D.Wang , F.Yi, and X.Li, "on general construction for extended visual cryptography schemes, " vol 41, pp 1410-1414, Apr 2008\

[18] J.Weir and W.yan, "Plane transform visual cryptography"Oct 2010, pp 60-74.

[19] C.Blundo, A.D.Santis, D.R.Stinson"on the contrast in visual cryptography schemes", j.cryptology, vol 12, pp 261-289

[20] C.N.Yang, "New visual secret sharing scheme using probabilisticmethod"vol 24 pp 484-494.