iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IX **Month of publication:** September 2019

DOI: http://doi.org/10.22214/ijraset.2019.9151

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue IX, Sep 2019- Available at www.ijraset.com

Secure and Efficient Steganography Scheme using 2-out-of-2 Secret Sharing Method

Shivam Singh[1], I B, Rajwade[2]
[1]*Student,* [2]*Assistant Professor , Department of Computer Science and Information Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Naini, Prayagraj – 211007*

Abstract: ***In this thesis we have proposed a scheme of steganography which is based on secret sharing. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information This paper proposes a secure and efficient steganography scheme using 2-out-of-2 secret sharing method. In the proposed approach secret shares are meaningful in nature which are less vulnerable for cryptanalysis. Secret messages are encrypted by the symmetric key in order to provide confidentiality even after extraction of the message. Both the shares are protected by the hash function in order to protect their integrity. Receiver can verify the authenticity of the shares and tamper location of the shares if share is tampered during transmission. Proposed approach is preserving all the security requirments like integrity, confidentiality, authenticity etc. Experimental results demonstrate the effectiveness of the proposed approach. Proposed approach provides good embedding capacity as well good tamper detection rate for the shares.***

Keywords-Secret sharing, Steganography, Self authentication, Meaningful shares., Share authentication.

I. INTRODUCTION

Due to the rise of the Internet, cryptography was created as a technique for securing the multimedia objects like Image, audio, video etc. There are basically three types of image based security approaches namely Visual cryptography or secret sharing, digital image watermarking and steganography. In this paper we have proposed a scheme of steganography which is based on secret sharing.

Secret sharing is very important branch of Visual Cryptography (VC). Secret may be image, speech or video. In this paper gray scale image has been taken in our consideration. When an image is transmitted via internet then it is very necessary to encode the image so that only an authority with valid decryption secret key can only take enjoy of that secret image. In this paper fundamental of visual cryptography is used to encode an image.

Visual cryptography (VC) is a technique for secret sharing, which is first proposed by Naor et al. [11]. VC permits the decryption of concealed images without the help of any computation. In a k-out-of-n visual secret sharing (VSS) scheme, an image is encoded into the form of n number of random shares. Random share means each share looks like an unsystematic binary pattern. Finally the shares are then printed onto transparencies.These transparencies will be treated like a secret key and will distributed among n participants. Since isolated share has no information related to secret image but one can see the secret visually by just stacking any k or more transparencies of the shares without any calculation. Infinite computation power can also not be able to decode the secret with, $k - 1$ or fewer participants. There are many other applications like access control, copyright protection [12], watermarking, identification [13] and visual authentication where visual cryptography could be used. One can understand the method of VSS by following example:

Consider a trivial 2-outof- 2 Visual secret sharing ($k = 2; n = 2$) scheme shown in Figure. 1. Each pixel p of secret binary image is encoded into a pair of black and white sub pixels for both shares. If p is white/black, one of the first/last two columns tabulated under the white/black pixel in Fig. 1 is selected randomly so that selection probability will be 50%. Then, the first two subpixels in that column are alloted to share 1 and the following other two subpixels are alloted to share 2. Irrespective of the color of the pixel whether black or white, it is encoded into two subpixels of black-white or white-black with equal probabilities. Thus single share can not decide whether the given pixel p is black or white . stacking of both the shares are shown in the last row of Fig

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue IX, Sep 2019- Available at www.ijraset.com

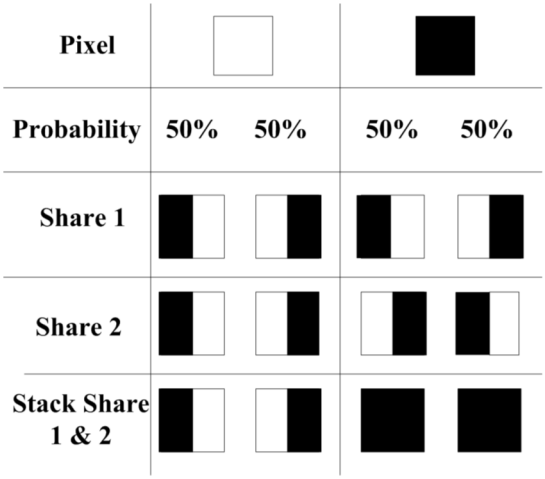


Fig. 1. Codebook for 2-out of 2 VSS scheme.

Black pixel p in input secret image leads two black sub pixels as an output which corresponds to a grey level 1. Whereas white pixel p in input secret image leads one black and one white sub pixels as an output which corresponds to a grey level 1/2.Thus by this way one can obtain the complete pseudo visual information without recovering the all pixels.

One can see the drawbacks of the existing secret sharing approach that are:

1) One cannot share non binary images by this rule.
2) One cannot be able to recover the complete secret image with full accuracy
3) Shares are expended in their size which is major drawback.

So, In this paper we have considered all these issue in our account and developed a novel approach which will be able to secretly share a gray scale image with meaningful shares without pixel expansion.

Due to latest advancements in the multimedia technology, image may be very easily altered. Verifying the integrity of the image is a very vital issue in many areas like court evidences There are various good multimedia alteration tools available nowadays by which tampering of the images are very easy task. Hence declaration for the authenticity of multimedia content is an important topic of concern for current era [3]. Image hashing is one of the technique which is the result of prevention approach for this type of alteration .Fragile watermarking is also a very good approach to ensure the integrity of the any given multimedia content.Watermarking not only allows to check the integrity of the given image , but also it is used to provide the ownership assertion of the given images. Image hashing maps an input image to a short string, called image hash, and has been widely used in image retrieval [1], image authentication [4],digital watermarking [5], image copy detection [6], tamper detection [7], image indexing [8], multimedia forensics [9],and reduced-reference image quality assessment [10].In the proposed approach, we have used self authentication method in order to protect the integrity of the shares. A teniese et al. [14] proposed the method of extended visual cryptography (EVC). In EVC, the shares contain both, shares are meaningful in nature but secret images can still be exposed only when qualified shares are stacked together. Shares of EVC scheme, however, provide very low visual quality as they are restricted only for binary images. Nakajima et al. [15] improved the current form of EVC approach for gray scale images in order to provide more visually appealing images. Shyongjian [16] proposed a visual cryptography approach for color images but he suffered with problem of share randomness. To make meaningful shares, A Halftone Visual Cryptography (HVC)is proposed by Zhou and Arce [18], which is more improved version of EVC.The main drawback of HVC approach is the pixel expansion. Zhonmin et al. [17] has proposed more extended version of HVC in which complimentary shares is replaced by the Auxiliary Black Pixel(ABP). Another time the short coming of this approach is pixel expansion.

Steganography is different from cryptography. In cryptography we focus on keeping the contents of a information secure, but in steganography we focus on making the existence of a message secure [19]. Both the techniques: Steganography and cryptography are individually sufficient to protect the information from unauthorized access.

The purpose of steganography is partly defeated [19] if steganalysis is successfully performed that is suspicion of the presence of the secret message. One can enhance the strength of the steganography by combining it with secret sharing .

Watermarking and hash functions are also a similar approach which are used to protect the secret message [20]. These technologies are mainly focused on the protection of the multimedia objects, but the approaches for these are entirely different from the secret

©IJRASET: All Rights are Reserved

sharing and steganography. The requirements of an efficient steganographic algorithm are good embedding capacity, less chance of steganalysis and good imperceptibility after embedding. Basically the objective of the watermarking approach is to provide copyright protection and image authentication [21]. Fingerprinting is also an approach which are generally used to track unique copies of the object which are going to be supplied to different customers. By this way a trusted third party can revoke the licence of the distribution authority [20]. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial [19]. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [20].

Steganography became famous only because of the certain loopholes in the existing cryptography approaches. Because of many rules provided by the government, strength of cryptography became more weaker [22][23], hence the focus of researchers are transferred to other security mechanism.

Hiding information behind the any meaningful images are less suspicious than other method.

Hence his paper intends to provide a novel and efficient algorithm for steganography approach. The power of the proposed method is enhanced using secret sharing method and hash function together.

Organization of the paper is as follows:

Section 2 deals with the various steps of the proposed approach. Experimental results and analysis are discussed in section 3. Paper is concluded in section 4, followed by references.

II. PROPOSED APPROACH

Propose approach is divided into six major steps as shown in figure 2. First three steps are handled at the sender side whereas last three steps are handled at receiver side. First of all we preprocess the secret message for efficient embedding into the images. In next step we create two meaningful shares using 2-out-of-2 secret sharing scheme which carries the secret message. After that to secure the secret share we apply hash function so that shares can authenticate themselves. These all three steps are incorporated at the sender side. Once the shares are transmitted we check for integrity of the shares at the receiver end. After that we extract the encrypted messages from the shares and then we decrypt it and save in a separate file to process further.

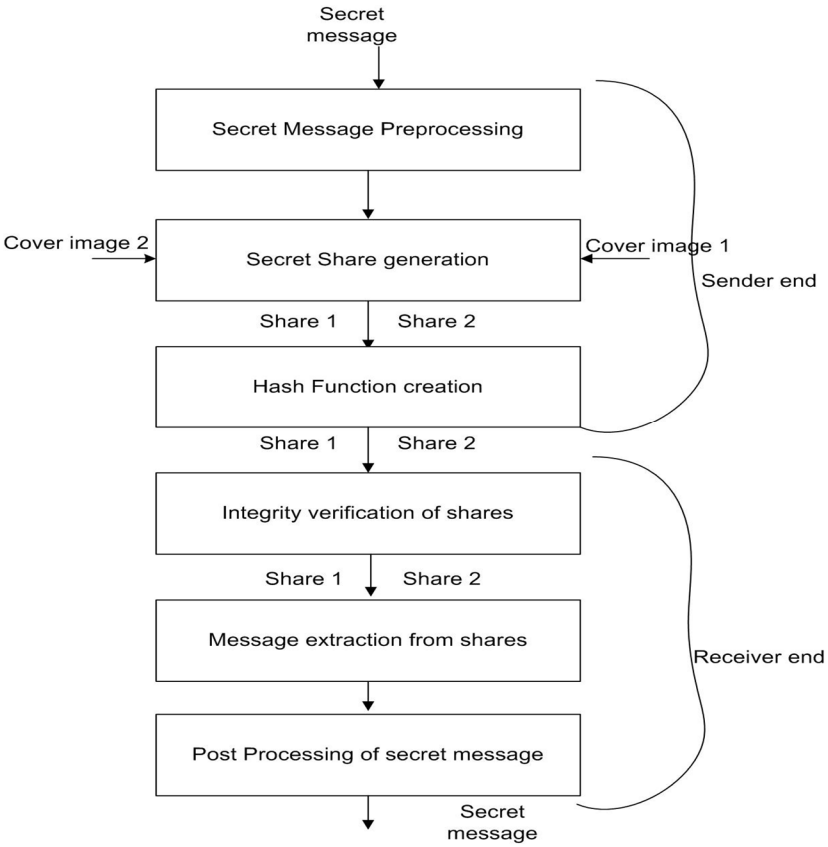


Figure 2- Flow Diagram of Proposed approach

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue IX, Sep 2019- Available at www.ijraset.com

A. Secret Message Pre-Processing

In this step, we take any text message directly or using text file which we want to secretly transmit using steganography as input. Our objective in this step is to preprocess this text message in such a way that it become more easier to handle and embed into images. There are following steps to do this job.

1) *Step 1:* Take a text message which may includes alphanumeric character or take a text file as input.
2) *Step 2:* Convert all characters into their ASCII values.
3) *Step 3:* Now convert these ASCII values into their eight bit binary format.
4) *Step 4:* Encryptthe entire binary bit stream using a symmetric key*k*.

$$E_s = Encrypt(Secret, k)$$

5) *Step 5:* Covert the scrambled bit stream into decimal format using the sets of eight binary bits.
6) *Step 6:* Create a matrix of size 128 × 128 using vector of scrambled ASCII values.

Now this is the pre-processed secret message which will be forwarded to next step.

B. Secret Share Generation

Once we get the encrypted secret message, we need to hide it into the image. In the proposed approach we are using the concept of secret sharing for hiding the secret message.

Here we are using two cover images which will act like shares. The equal proportion of the bit depth of secret pixel will be embedded into both the shares, so that no individual share will have the full access to the secret. When both the shares will combine together then only one can get the secret image. Following steps are required to embed the secret message into the both the shares:

1) *Step 1:* Take the encrypted secret message E_s meaningful Shares S_1 and S_2 as input.
2) *Step 2:* Convert each decimal secret value into the eight bit binary bit stream*b*.
3) $b_i = binarize(E_s) Where\ i = 1\ to\ 8$
4) *Step 3:* Divide each share into non overlapping blocks of size 2 × 2.
5) *Step 4:* Extract first four LSBs of b_i of secret message's first character and assign it to second LSBs of each pixel of first block of S_1similarly last four LSBs will be assigned to second LSBs of each pixel of first block of S_2.
6) *Step 5:* Repeat step 4 for each character of E_s.

Using this method only one bit of each pixel of the share will be affected. Because we are just modifying the single LSBs of each pixel in the block and each block contain four pixels and we have two blocks (of two shares) for single secret character of E_s. It means 4 × 2 = 8 bits can be accommodated by destroying only single bit of each pixel of the shares.

After embedding all the encrypted characters of E_s finally we get the secret shares. The beauty of these shares are that these are meaningful in nature as well as insufficient share will never reveal the secret. As we know that proposed approach is 2-out-of-2 secret sharing scheme hence we need exactly two shares at the receiver end in order to reveal the secret.

C. Hash Function Generation

This step is required in order to secure the shares. We apply hash function on each share so that receiver can verify the integrity of shares at the receiver end.

It is quite possible that a share may be altered during transmission because of any intentional or unintentional attack. So by this way receiver can check whether the shares are tampered or not. If shares are tampered then receiver can ask to sender for newer version of the shares else he will continue with the same set of shares. Following steps are required to perform this module:

1) *Step 1:* Apply first hash function on first seven bits (excluding first LSB) of each pixel of the share 1 which will return a single bit. This hash function will be generated by symmetric key k_1.

$$h_1 = Hash1(b_{8to2}, k_1)$$

2) *Step 2:* This bit h_1 will be generated for each pixel of share S_1 and it will be embedded into the first LSB of each pixel.
3) *Step 3:* Apply second hash function on first seven bits (excluding first LSB) of each pixel of the share 2 which will return a single bit. This hash function will be generated by symmetric key k_2.

$$h_2 = Hash2(b_{8to2}, k_2)$$

4) *Step 2:* This bit h_2 will be generated for each pixel of share S_2 and it will be embedded into the first LSB of each pixel.

©IJRASET: All Rights are Reserved

D. Integrity Verification of Shares

This step is executed on the receiver side. When receiver receives the shares then first of all he will check the authenticity and integrity of the shares. If both the shares will be unaltered then only he will proceed further else he will ask to sender for the new shares. Receiver will follow the steps mentioned below:

1) *Step 1:* Extract first LSB of each pixel of share $S_1$and make a separate binary matrix M_1 of same size.
2) *Step 2:* Recalculate the hash function 1 on the seven bits of each pixel of S_1 using the same symmetric key k_1. Now we will get h_1 for each pixel. Hence create another binary matrix M_2using h_1.
3) *Step 3:* Compare both the binary matrix. If there is any mismatch then mark that pixel as altered one.T_1 is the matrix which shows the location of tampered pixels.

$$T_1(i,j) = \begin{cases} 1, & M_1(i,j) \neq M_2(i,j) \\ 0, & M_1(i,j) = M_2(i,j) \end{cases}$$

4) *Step 4:* Extract first LSB of each pixel of share S_2 and make a separate binary matrix M_1 of same size.
5) *Step 5:* Recalculate the hash function 2 on the seven bits of each pixel of S_1 using the same symmetric key k_2. Now we will get h_2 for each pixel. Hence create another binary matrix M_2using h_2.
6) *Step 6:* Compare both the binary matrix. If there is any mismatch then mark that pixel as altered one. T_2 is the matrix which shows the location of tampered pixels.

$$T_2(i,j) = \begin{cases} 1, & M_1(i,j) \neq M_2(i,j) \\ 0, & M_1(i,j) = M_2(i,j) \end{cases}$$

E. Message Extraction From The Shares

Once we check the integrity of the shares, and if share is authentic then we need to extract the secret information from the each share. Following steps are required to extract the message:

1) *Step 1:* Divide the each share in to non overlapping blocks of size 2×2.
2) *Step 2:* extract second LSB of each pixel from four pixels of each block.
3) *Step 3:* Now we have total eight bits (four from block of first share and four from the corresponding block of second share). Append these bit streams for each block.

F. Post Processing Of The Secret

As we have embedded the encrypted binary bits into the shares so that message could not be read by unauthorized person even after extraction hence we need to decrypt it at receiver end. Following steps will be taken to do the same.

1) *Step 1:* Apply the same symmetric key *k* in order to decrypt the encrypted binary bits.

$$S = Decrypt(E_s, k)$$

2) *Step 2:* Convert all the sets of eight bit binary bit streams into corresponding decimal format.
3) *Step 3:* These all the decimal values are nothing but the ASCII values of the secret character. Now convert these ASCII values into the corresponding alphanumeric character. These character stream is the actual secret message.

III. EXPERIMENTAL RESULT AND ANALYSIS

Proposed approach has been implemented in MATLAB 2015, window 7 (operating system)with processor intel core 2 duo . Experimental results show two meaningful shares for a gray scale secret image and which are embedded with the textual secret message. Experimental results also shows the integrity verification for the shares.

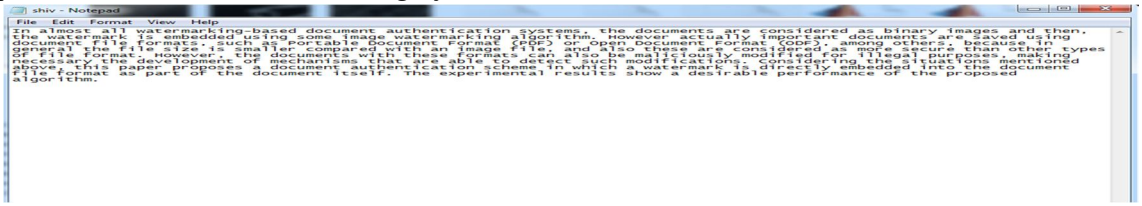


Figure 2: Example of the text file.

Figure 2 shows the example of the secret text file which contains quite general type of text message including alphanumeric character with special character.

©IJRASET: All Rights are Reserved

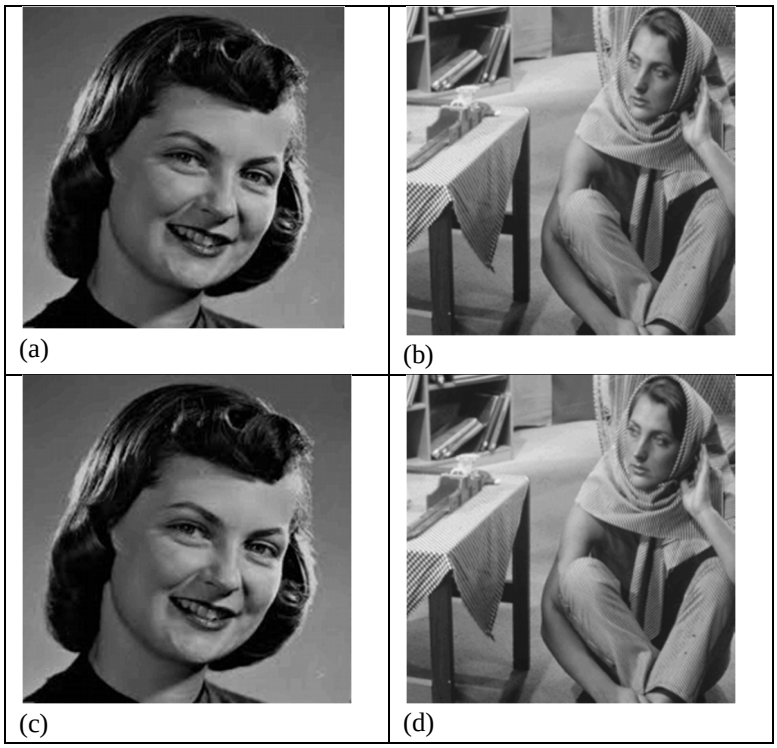


Figure 3- Example of Meaningful shares used for embedding of secret message

Figure 3 demonstrate the results of secret embedding and meaningful share generation. Figure 3(a) and (b) are the cover images which will be acted like meaningful shares and secret will be embedded into it. Figure (d) and (e) are the meaningful shares after embedding. E can see visually that there is both the images imperceptibly looking fine with respect to the original image. We have verified the imperceptibility by using PSNR values and it is satisfactory as shown in table 1.

Table 1- Imperceptibility of the shares

Share Image	Amount of secret (%)	PSNR (dB)
Girl	35%	46 dB
Barbara	35%	42dB
Girl	60%	33 dB
Barbara	60%	37dB
Girl	75%	20 dB
Barbara	75%	22 dB

In table 1, we can see that as we are increasing the embedding percentage our imperceptibility is decreasing accordingly. But still we are able to hold a satisfactory amount of imperceptibility.

©IJRASET: All Rights are Reserved

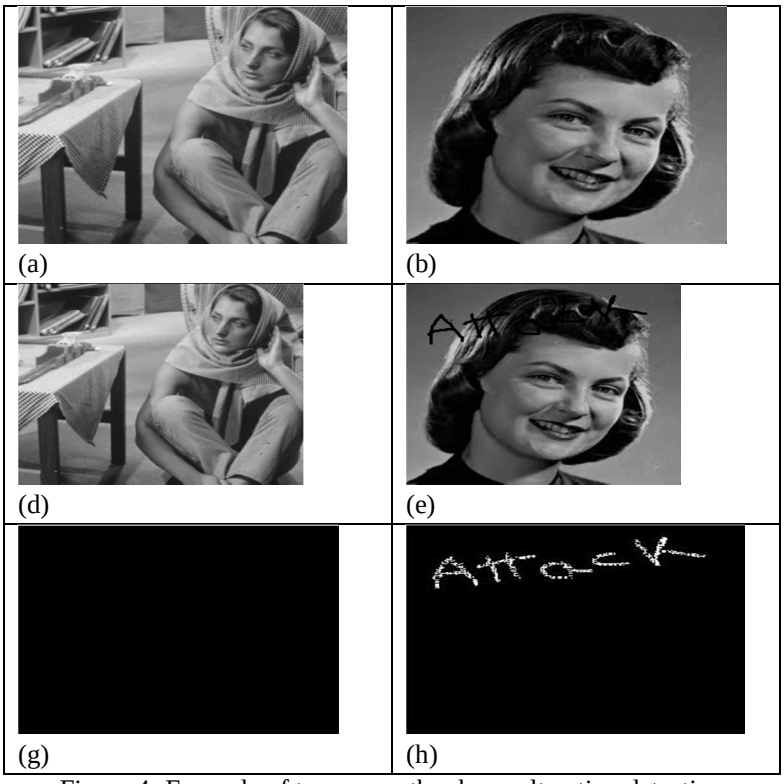


Figure 4- Example of tamper on the share, alteration detection

Figure 4 demonstrates the effectiveness of the proposed approach for the alteration detection of shares. Here we can see that figure (a) and (b) are the meaningful shares with fully embedded with the secret. These shares are also protected with the hash function. In this experimental result we are just checking the effectiveness of the hash function. It means, whether we are able to detect the alteration or not.

Let us consider that an attacker has done some intentional attack (written some objectionable text on the shares) on share 2 and left the share 1 as it is as shown in figure (d) and (e). Now at the receiver side, there is no information related to the original shares. Receiver has only tampered share.

This is a challenge for the receiver that only with the help of tampered shares, he has to confirm that the shares are not authentic. Receiver will apply our algorithms in order detect the alteration. Figure (g) and (h) are the results of tamper detection. Here black pixels show the unaltered region whereas white pixels show the altered one. As share 2 is altered hence we can see the tamper detection in the corresponding figure (h). Here we can see that we are not getting complete white pixels for the tamper detection this scenario is called false rejection. Once the receiver will identify that a particular share is unauthentic then he will ask to the sender to send the corresponding share. Table 2 demonstrates the quantitative analysis for the tamper detection capabilities for the proposed approach. Here one can observe that we are getting very good accuracy for the alteration detection.

Table 2- Tamper detection results for shares.

Secret Image	Altered pixel in Share 1	Altered pixel in Share 2	Detected Pixels in Share 1	Detected Pixels in Share 2
Girl	200	0	186	0
Barbara	498	587	498	520
Lena	321	631	302	601
Cameraman	492	204	403	184
Boat	283	102	251	91
House	541	309	510	261

©IJRASET: All Rights are Reserved

So by the observation of the experimental results, one can conclude that proposed approach has good level of embedding capacity for the secret message.

Due to block based embedding, we are also achieving satisfactory range of imperceptibility with respect to original image of the share. Meaningful shares are less vulnerable for cryptanalysis. Tamper detection rate is also good for the shares in case of any intentional or unintentional attacks.

IV. CONCLUSION

In this paper a secure and efficient steganography scheme using 2-out-of-2 secret sharing method is proposed. In the proposed approach a secret document containing alphanumeric characters are saved in two shares. These two shares are meaningful in nature in order to avoid the vulnerability against cryptanalysis.

Using block based embedding technique the embedding capacity is increased. Peak signal to noise ratio is used to ensure the good quality of imperceptibility.

Both the meaningful shares are protected using two different hash function in order to protect their integrity. Receiver can verify the authenticity of the shares and tamper location of the shares if share is tampered during transmission intentionally or unintentionally. Experiments are carried out in order to demonstrate the effectiveness of the proposed approach. Tables are shown to provide the quantitative results of imperceptibility and tamper detection.

V. ACKNOWLEDGEMENT

I express profound sense of gratitude to my advisor Mr. I.B Rajwade Assistant Professor, Department of Computer Science and Information Technology, SHUATS, Prayagraj whose guidance, motivation and invaluable support in providing the opportunity to conduct my thesis. He brought aspects to my attention that I had to improve and continue to work on.

I would also like to thank Er. Sanjay T.Singh and Er. Rishabh Chaudhary Assistant Professor, Department of Computer Science and Information Technology, SHUATS for making the supportive work environment.

I would also like to take opportunity to thank Dr. H. M. Singh, Assistant Professor, Department of Computer Science and Information Technology, SHUATS, for providing the knowledge that opened the new horizon by his special teaching style.

I would also like to take opportunity to thank Dr. W. Jeberson, Head of the Department, Department of Computer Science and Technology, SHUATS,for his consistent help in making the thesis.

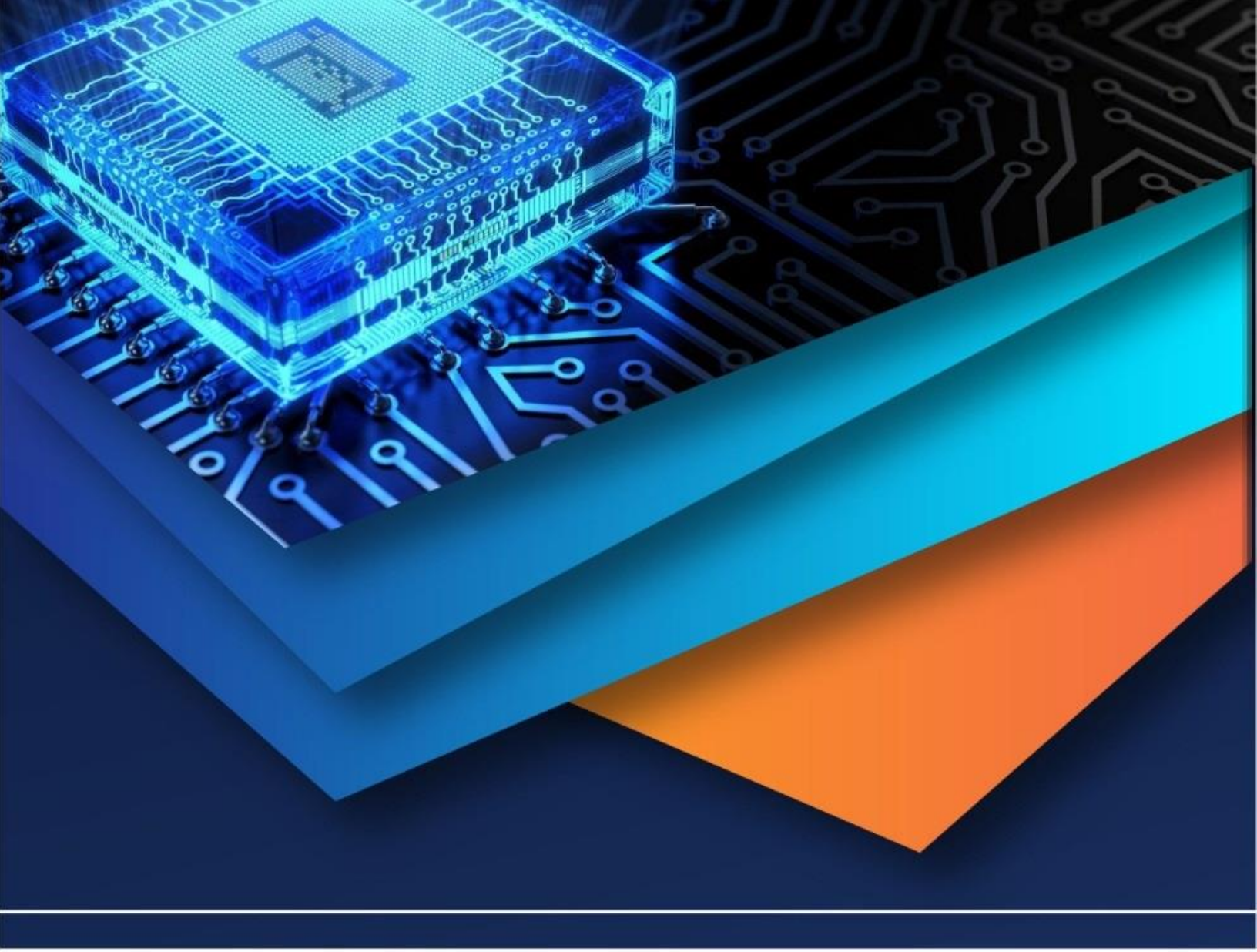
REFERENCES

[1] M. Slaney and M. Casey, “Locality-Sensitive Hashing for FindingNearest Neighbors,” IEEE Signal Processing Magazine, vol. 25,no. 2, pp.128-131, Mar. 2008.
[2] M.N. Wu, C.C. Lin, and C.C. Chang, “Novel Image CopyDetection with Rotating Tolerance,” J. Systems and Software,vol. 80, no. 7, pp. 1057-1069, 2007.
[3] S. Wang and X. Zhang, “Recent Development of Perceptual ImageHashing,” J. Shanghai Univ. (English ed.), vol. 11, no. 4, pp. 323-331,2007.
[4] F. Ahmed, M.Y. Siyal, and V.U. Abbas, “A Secure and RobustHash-Based Scheme for Image Authentication,” Signal Processing,vol. 90, no. 5, pp. 1456-1470, 2010.
[5] C. Qin, C.C. Chang, and P.Y. Chen, “Self-Embedding FragileWatermarking with Restoration Capability Based on Adaptive BitAllocation Mechanism,” Signal Processing, vol. 92, no. 4, pp. 1137-1150, 2012.
[6] C.S. Lu, C.Y. Hsu, S.W. Sun, and P.C. Chang, “Robust Mesh-BasedHashing for Copy Detection and Tracing of Images,” Proc. IEEEInt’l Conf. Multimedia and Expo, vol. 1, pp. 731-734, 2004.
[7] Z. Tang, S. Wang, X. Zhang, W. Wei, and S. Su, “Robust ImageHashing for Tamper Detection Using Non-Negative MatrixFactorization,” J. Ubiquitous Convergence and Technology, vol. 2,no. 1, pp. 18-26, 2008.
[8] E. Hassan, S. Chaudhury, and M. Gopal, “Feature Combination inKernel Space for Distance Based Image Hashing,” IEEE Trans.Multimedia, vol. 14, no. 4, pp. 1179-1195, Aug. 2012.
[9] W. Lu and M. Wu, “Multimedia Forensic Hash Based on VisualWords,” Proc. IEEE Int’l Conf. Image Processing, pp. 989-992, 2010.
[10] X. Lv and Z.J. Wang, “Reduced-Reference Image Quality AssessmentBased on Perceptual Image Hashing,” Proc. IEEE Int’l Conf.Image Processing, pp. 4361-4364, 2009.
[11] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptograhy: EUROCRYPT94, LNCS, vol. 950, pp. 112, 1995.
[12] M. S. Fu and O. C. Au, “Joint visual cryptography and watermarking,” in Proc. IEEE Int. Conf. Multimedia and Expo, Taipei, Taiwan, Jun. 2004.
[13] M. Naor and B. Pinkas, “Visual authentication and identification,” Crypto97, LNCS, vol. 1294, pp. 322340, 1997.
[14] Ateniese G, Blundo C, De Santis A, Stinson DR (2001) Extended capabilities for visual cryptography.TheorComputSci 250:143–161
[15] Nakajima M, Yamaguchi Y (2002) Extended visual cryptography for natural images. In: J. WSCG,vol 10, pp 303–310
[16] Shyu SJ (2007) Image encryption by random grids. PattRecog 40(3):1014–1031
[17] Wang Z, Arce GR, Crescenzo GD (2009) Halftone visual cryptography via error diffusion. IEEE TransInf Forensics Secur 4(3):383–396
[18] Zhou Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. IEEE Trans Image Process15(8):2441–2453
[19] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM,47:10, October 2004
[20] Anderson, R.J. &Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areasin Communications, May 1998

©IJRASET: All Rights are Reserved

[21] Marvel, L.M., Boncelet Jr., C.G. &Retter, C., "Spread Spectrum Steganography", IEEE Transactionson image processing, 8:08, 1999
[22] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANSInstitute, January 2002
[23] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June
[24] Emam, M. M., Aly, A. A., &Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications, 1(7), pp. 361-366, (2016).
[25] Pandit, A. S., Khope, S. R., & Student, F. Review on Image Steganography. International Journal of Engineering Science, 6115, (2016).
[26] Cis.upenn.edu, 'Encryption and Steganography', 2015. [Online]. Available: http://www.cis.upenn.edu/~cis110/13fa/hw/hw04/steganography.html#steganography. [Accessed: 04- May- 2015].

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)