

A Hybrid Approach for Image Protected Shares Based on Visual Cryptography and Fragile Watermarking Scheme

Surendra Kumar Raut

Department of Computer Science and Engineering
MNNIT Allahabad-211004
Allahabad, India
bana.surendra@gmail.com

Durgesh Singh

Department of Computer Science and Engineering
MNNIT Allahabad-211004
Allahabad, India
durgeshcse@gmail.com

Shivendra Shivani

Department of Computer Science and Engineering
MNNIT Allahabad-211004
Allahabad, India
shivendrashivani@gmail.com

Suneeta Agarwal

Department of Computer Science and Engineering
MNNIT Allahabad-211004
Allahabad, India
suneeta@mnnit.ac.in

Abstract— In Visual Cryptography (VC), shares are the most sensible objects and may be tampered by any unauthorized person. So the protection of VC shares is most essential. This paper proposes a hybrid approach in which shares of VC are protected through the self embedding fragile watermarking technique. At the receiver end, these protected shares are checked for any alteration by recalculating watermark and comparing with the existing watermark in protected shares. If any mismatch is found, altered pixels are marked so that receiver can request the sender to retransmit the particular shares, otherwise shares will be stacked together after discarding the watermark and recover the secret image.

Keywords— Visual Cryptography, Fragile Watermarking, Self Embedding, Protected Shares.

I. INTRODUCTION

Nowadays, transfer of multimedia data, medical image etc. are very common through Internet. With the coming trends of multimedia and electronic commerce, there is a vital need to solve the problem of ensuring information safety in today's increasingly open network environment. The traditional cryptography is usually used to protect information security. Data become disordered after being encrypted with such technologies and then can be recovered by decryption with a correct key. It is very rare to recover the encrypted source content without the key by unauthorized persons who intend to steal the data.

In 1994, Naor and Shamir [1] proposed a new cryptography area, Visual Cryptography (VC). It is a secret sharing technique used for sharing of visible object (i.e. text, image etc.) secretly. The most notable feature of this approach is that it allows the

retrieval of the secret information without any cryptographic computation because decryption is done by human visual system only. In this technique secret information is distributed in the form of shares to different users. Each share shows nothing more than a random binary pattern which does not reveal any information about the secret. The secret information can be recovered only when all the distributed shares are collected together and stacked on top of one another. Two parameters basically influence the effectiveness of Visual Cryptography that is contrast and pixel expansion. Visual Cryptography technique has many variants these are as follows [4]:

1. **2-out-of-2 VC (2, 2):** It is the simplest Visual Cryptography scheme where secret image is encrypted into two shares and the secret image is recovered only after two shares are stacked. Single share does not reveal any information about the secret image.
2. **2-out-of-n VC (2, n):** In this Visual Cryptography scheme secret image is encrypted into n shares, each share is random binary share which do not reveal any information about the secret image. Secret image is visible after stack of two or more than two shares.
3. **n-out-of-n VC (n, n):** In this Visual Cryptography scheme secret image is encrypted into n shares (participants), each share is random binary share which does not reveal any information about the secret image. Secret image is visible after stack of all the n shares (Qualified set). If less the n shares (forbidden set) are stacked secret image is not recovered.

4. **k-out-of-n VC (k, n):** It is the generalized one. In this scheme n shares are generated from the secret image each does not reveal any secret. To recover secret image at least k shares are required for stacking. Less than k shares are unable to recover the secret image.

A 2-out-of-2 Visual Cryptography (two shares for secret image) uses two bits pixel expansions, i.e. for any single pixel of secret image there are two sub pixels in each share for a binary image [5].















Pixel				
Probability	50%	50%	50%	50%
Share 1				
Share 2				
Stack 1 & 2				

Fig. 1. Block diagram of 2-out-of-2 VC scheme.

Each pixel of binary image is encoded into black and white sub pixels. Let P be a pixel of secret binary image, P will be expanded into two sub pixels (one white and one black) in each two shares with equal probability. So, individual share does not give any clue whether the pixel is black or white. If the pixel is white pixel then any combination of second column of Fig.1, is chosen with 50% probability. If the pixel is black then any combination from column3 is chosen with 50% probability. As it is shown in the last row of the Fig.1 (result after stacking two shares), if the pixel is white, then after superimpose of two shares in the corresponding two sub pixels one will be black and one white, i.e. half gray value. If the pixel is black pixel then corresponding two sub pixels will be black after stacking. So, for black pixel there are two black sub pixels but for white pixel there is one black, one white sub pixel i.e. half gray value, so there is 50% contrast loss in the resultant image.

Digital watermarking is a process for inserting watermark (ownership information or hidden information or mark) into cover signal such as audio or image data. At any given moment, the hidden information can be extracted to prove ownership or to ensure integrity or simply to get some copyright-related information. Image, text, video or any logo which can be notified as courtroom evidence can be the ownership information. Watermark can be inserted in spatial domain as well as in the frequency domain. In Spatial method directly pixel value is changed but in the frequency domain image is first transformed and then watermark is inserted into transform domain. The spatial domain method is less robust to geometric distortions and less resistant to noise and compression. It is faster as transformation is not required

whereas transform domain method is more robust against image compression, image filtering etc. Digital watermarking technique can be categorized into three categories namely robust, fragile and semi fragile watermarking [3] [6]. In robust digital watermarking applications, the watermark is extracted even if modification is strong. However, extraction is failed in case of fragile watermarking. Fragile watermarking has come into picture for ensuring the legitimacy and data integrity [2][3]. Fragile watermarking can be achieved block-wise or pixel-wise depending upon insertion of the hidden information to the cover image.

The remaining paper is organized as follows: the proposed scheme is given in section II and in section III the experimental results are shown. The paper is concluded in section IV followed by the references.

II. PROPOSED ALGORITHM

The proposed approach has two phases. First one is encryption and second one is decryption. In the encryption, input secret image is encrypted into two protected shares based on self embedding fragile watermarking scheme while in decryption individual share is checked for any alteration. If any possible alteration (i.e. modification) is detected to the share, then the alteration is marked and shown as tampered share and receiver requests the sender to resend new genuine share, otherwise two shares are stacked together after discarding watermark information to get the secret image. Here Fig. 2 and Fig. 3 show the encryption procedure and the decryption procedure respectively.

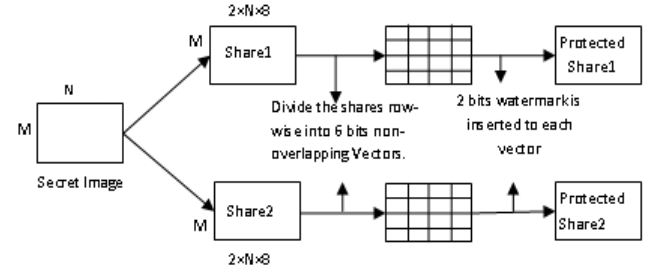


Fig. 2. Block diagram for encryption procedure.

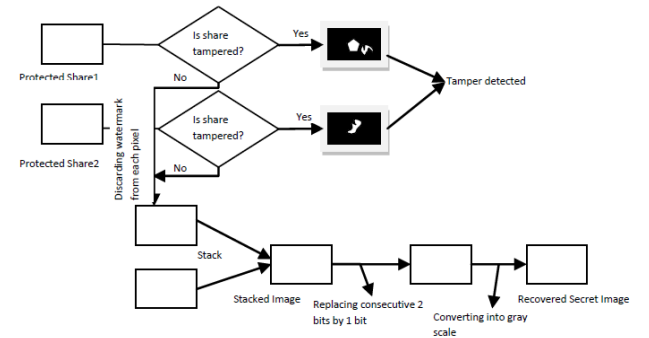


Fig. 3. Block diagram for encryption procedure.

A. Encryption Procedure

The encryption procedure consists of following steps:

Step-1: The gray value of each pixel of input image is converted into eight bit binary representation.

Step-2: Do two bits pixel expansion for each bit to generate shares using table 1. For example if the bit value is 1 in the image then, either (0, 1), (1, 0) or (1, 0), (0, 1) will be stored in share1 and share2 respectively.

TABLE I. Pixel Expansion encoded

	For bit values 1		For bit values 0	
Share1	0 1	1 0	0 1	1 0
Share2	1 0	0 1	0 1	1 0
After stack	1 1	1 1	0 1	1 0

Step-3: To generate protected shares, divide each share row wise into six binary bits non-overlapping vectors. Now calculate the two binary bits watermark information for each vector. These two bits generation procedures are as follows.

B. Bits Generation

Let the total number of 6-bits vectors in each share be S. Individual binary bit of a vector B_p of share can be written as b_i where $i \in (0, \dots, 5)$ and $p \in (1, \dots, S)$, the position value of that vector i.e. the row value and column value in which the vector lies are denoted by G_p^r and G_p^c and the binary representation of G_p^r and G_p^c are $b_7^r b_6^r b_5^r \dots b_0^r$ and $b_7^c b_6^c b_5^c \dots b_0^c$ respectively.

Watermark bit₁ (T_{b1}) Generation:

Generate the *Watermark bit₁* in following manner:

$$X = Ex - OR(b_i^r, b_i), i = 5, 4 \dots 0 \quad (1)$$

$$Y = Ex - OR(b_i^c, b_i), i = 5, 4 \dots 0 \quad (2)$$

Where, X represents bitwise Ex-OR operation between 6 binary bits of each vector and 6 LSB of row value of the corresponding vector. Similarly Y represents bitwise Ex-OR operation between 6 binary bits of each vector and 6 LSB of column value of corresponding vector.

$$T_{b1} = \left(\sum_{i=1}^6 (X_i \times Y_i) \right) \bmod 2 \quad (3)$$

Watermark bit₂ (T_{b2}) Generation:

This bit for each vector can be calculated from six binary bits of that vector itself. First we will make the pair of each two consecutive bits and take the Ex-OR operation of bits of each pair, so there will be five bits, then add all the five bits and take mod 2 operation of the sum of the five bits.

$$T_{b2} = \left(\sum_{i=0}^5 (b_i \oplus b_{i+1}) \right) \bmod 2 \quad (4)$$

After calculating two bits watermark for each vector of the shares, convert these eight bits (i.e. six binary bits of each vector and two bits corresponding watermark, T_{b1} as first LSB and T_{b2} as second LSB) into single gray scale pixel for each vector and called them as protected shares. Finally these protected shares will be transmitted to the receivers.

C. Decryption Procedure

Protected share1 and protected share2 are first checked for alteration, If any alteration is made to the shares then the alteration is marked and shown as tampered one, otherwise shares are stacked and the original secret image is recovered. This decryption procedure can be done in following:

Step-1: Using six MSBs of each pixel of protected shares recalculated T_{b1} and T_{b2} using equation 3 and equation 4, and match with first and second LSB of that pixel. If any mismatch is found then that pixel treated as altered one otherwise treated as unaltered.

Step-2: If the protected share1 and/or protected share2 is/are altered, then the portions where alteration (corresponding pixel) are marked and shown as tampered share so that receiver can request sender to resend new genuine share.

Step-3: If the Protected share1 and protected share2 are unaltered, then these two shares are bitwise stacked after removing watermark data and resulting image known as stack image. This stack image is binary image.

Step-4: Replace the consecutive two bits of the stack image by one bit using table II. For example, set the value by zero, if two consecutive bits differ otherwise set value by one. The resulting image will be of size of $M \times 8N$ and convert this into the corresponding gray scale image and get the original secret image.

TABLE II. Pixel decoded in shares

Consecutive two bits	Decoded bit
1 1	1
1 0	0
0 1	0

III. EXPERIMENTAL RESULTS

To show the efficiency and accuracy of this approach, we demonstrate it with the help of 4 examples as shown in Fig. 4. Images of size 256×256 are taken from the standard image database like Baboon, Lena, Vegetable and Cameraman. For each image, two protected shares, protected share1 and protected share2 are generated. In the tampered detection column of Fig. 4, white region shows altered pixel whereas black region shows unaltered one. In the first example Baboon image is taken. Protected share1 is tampered (VC is written inside it) and protected share2 is unaltered. At the receiver end this tampering is detected. So, the receiver can inform the sender about this tampering and can request the sender to resend the genuine share. In the second example Lena image is taken. Both protected shares are tampered and these are detected accurately at the receiver end before stacking of the

shares. In the third example Vegetable image is taken. Shares are tampered by addition of ‘paper and salt’ noise of matlab library. This noise is in the form of small dot in the image which is less visible but this is still detected by our algorithm accurately. In the fourth example Cameraman

image is taken. Here no share is tampered, so after the detection algorithm, two black images are shown at the receiver end. Next both shares are stacked together to recover the secret image as shown in the Fig. 5.

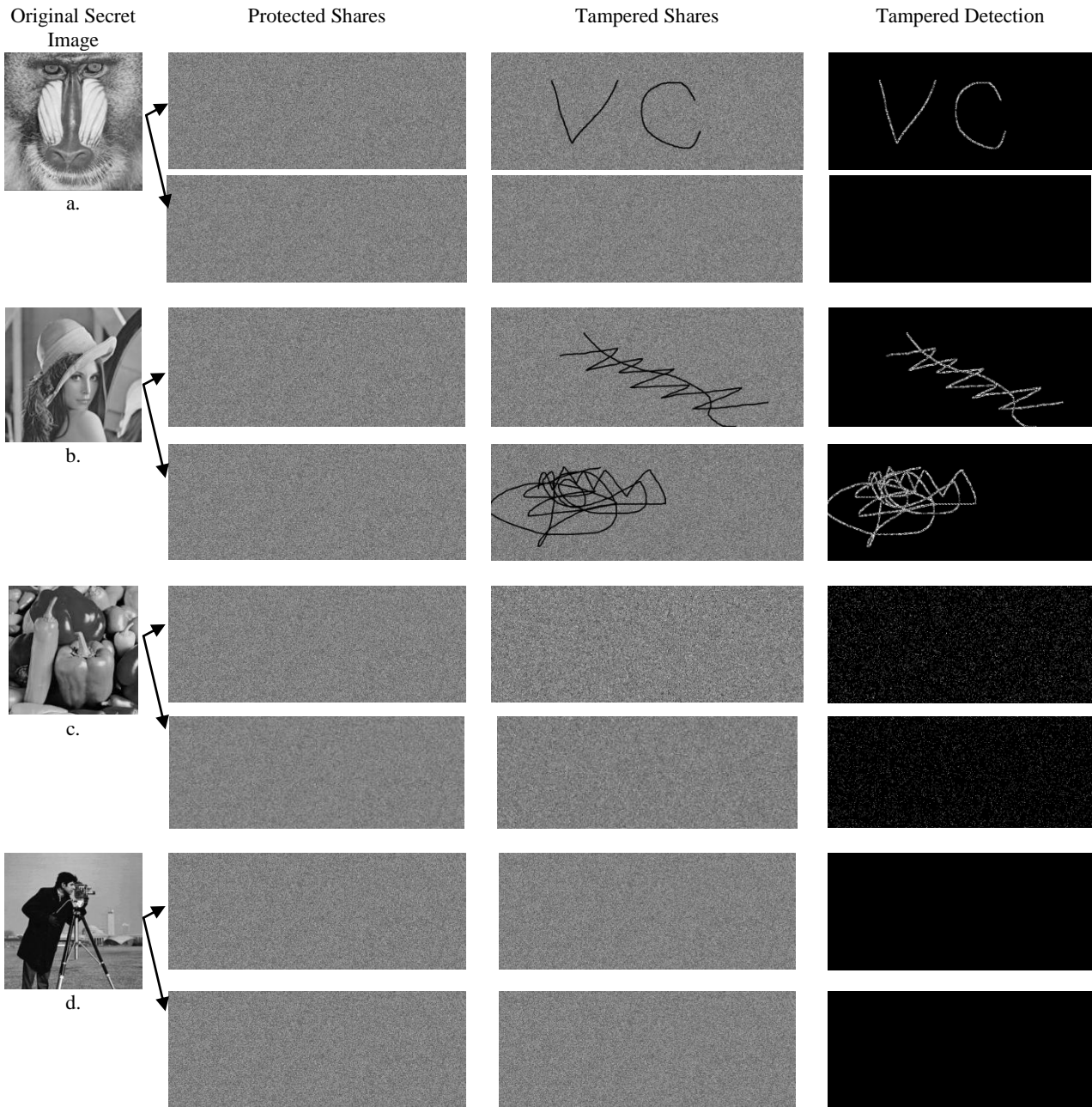


Fig. 4. a. Baboon b. Lena c. Vegitable d. Cameraman Image

Original Secret Image



Recovered Image



Fig. 5. Cameraman Recovered Image

The observation during experimental results is shown in table III in which we can see the number of altered pixels in both shares for various images along with their detection rate. The detection rate is very high which shows the efficiency of our proposed approach.

Table III: Essential information observed during encryption and decryption of VC

Secret Image	No. of Altered Pixels	No. of Detected Pixels	Detection Accuracy (%)
Baboon	131	119	96.94
Lena	595	586	98.48
Vegetable	2635	2689	97.99
Camera man	0	0	100

IV. CONCLUSION AND FUTURE WORK

This paper suggests an efficient approach which ensures the integrity of the shares made by Visual Cryptography using self embedding fragile watermarking scheme. At the receiver end, these protected shares are checked for any possible alteration by comparing the recalculated the watermark bits with the

extracted two LSBs of corresponding pixel of tampered shares. If any mismatch found it shows that the pixel has been altered, altered pixels are marked and shown so that receiver can request the sender to retransmit shares, otherwise shares will be stacked together to recover the secret image. The experiments have been performed on the wide set of standard image data set and different kinds of attacks. The rate of detection of altered pixels is very high. In future recovery of tampered shares can be done by adding some new features.

REFERENCES

- [1] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology Eurocrypt '94, Lecture Notes in Computer Science, Springer, Berlin, , Vol. 950, pp. 1–12, 1995
- [2] D. Singh, S. Shivani, S. Agarwal, "Self-embedding Pixel wise Fragile Watermarking Scheme for Image Authentication" in International Conference on Intelligent Interactive Technologies and Multimedia, Allahabad(IITM 2013), pp. 111-122, vol. 276, Springer CCIS, ISBN: 978-3-642-37463-0.
- [3] S. Shivendra, A. K. Patel, S. Kamble, S. Agarwal, "An effective pixel-wise fragile watermarking scheme based on ARA bits." In Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 221-226. ACM, 2011.
- [4] Y.Bani, Dr B. Majhi, and R. S. Mangrulkar. "A Novel Approach for Visual Cryptography Using a Watermarking Technique." In Proceedings of 2nd National Conference, IndiaCom, pp. 08-09. 2008.
- [5] Wang, Zhongmin, G. R. Arce, and G. D. Crescenzo. "Halftone visual cryptography via error diffusion." Information Forensics and Security, IEEE Transactions on 4.3 (2009): 383-396.
- [6] Zhou, H. Li, P. Yu. "Semi-fragile watermarking technique for image tamper localization." Measuring Technology and Mechatronics Automation, 2009. ICMTMA'09. International Conference on. Vol. 1. IEEE, 2009.