Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.185 – 193

RESEARCH ARTICLE

REVERSIBLE WATERMARKING FOR DIGITAL IMAGES USING VISUAL CRYPTOGRAPHY AND PIXEL HISTOGRAM SHIFTING

Naina Gaharwar[1]
Master of Engineering in Computer Engineering
Pd. Dr. D.Y.Patil Institute of Engineering and Technology, Pimpri, Pune-18, India
nainagaharwar@gmail.com

Prof. Dr. Reena Gunjan[2]
Professor in Computer Engineering
Pd. Dr. D.Y.Patil Institute of Engineering and Technology, Pimpri, Pune-18, India
reenagunjan@gmail.com

Abstract: ***There is a rapid growth in Internet technology so information can be exchanged quickly and easily over web. This information includes images, videos, audios and documents. Medical and military images have sensitive contents, for which any modification may impact their interpretation. This information needs to be protected. To protect this various techniques were developed. Watermarking is one of the techniques to protect images consisting of sensitive contents. In the field of watermarking a lot of research is taking place to establish more efficient reversible techniques. This paper proposes a watermarking scheme which offers better security than Hwang's method, so that, attackers will not be able to detect ownership information. The proposed scheme embeds the secret image without modifying the host image. In addition, Without using the original host image we can extract the hidden secret image and allows multiple watermarks to be embedded in the same image. The experimental results shows that the proposed scheme is robust to withstand several image processing attacks such as JPEG compression, noise adding, sharpening and blurring. This method reduces distortion and increases embedding capacity of research is taking place in the field of watermarking to establish more efficient reversible techniques. To improve the quality of the watermarked image a Pixel Histogram Shifting (PHS) is introduced. In this method the image is classified for finding watermark region and then watermark bits are applied by direct histogram shifting. Visual cryptography is used to provide more security to images.***

Keywords — Histogram Shifting, Reversible Watermarking, Visual cryptography

I. INTRODUCTION

Information is exchanged in text message during older days. Now-a-days, Information is being transferred as digital images, audios or videos etc. This gives a boost to the technology but at the same time multimedia transmission is insecure, as lot of hackers and attackers are there who can modify or duplicate the data. Thus there should be a technique to protect this data that are being transmitted. Most of the military and medicals records need a high security. These documents contains lot of confidential information which should not be exposed without the concerned person‟s permission. So, Watermarking method is developed to maintain integrity of data. Watermarking means hiding secret data with cover image, so the image is protected from external access. For about ten years, several reversible watermarking schemes have been proposed for protecting images of sensitive content, like medical or military images, for which any modification may impact their interpretation [1]. These methods allow the user to restore exactly the original image from its watermarked version by removing the watermark.

Thus to update the watermark content is possible now, as for example security attributes (e.g., one digital signature or some authenticity codes), at any time without adding new image distortions. Once the watermark is removed, the image is not protected. So, even though watermark removal is possible, as most applications have a high interest in keeping the watermark in the image as long as possible its imperceptibility has to be guaranteed, taking advantage of the continuous protection watermarking offers in the storage, transmission and also processing of the information [2]. This is the reason why, there is still a need for reversible techniques that introduce the lowest distortion possible with high embedding capacity. Various methods have been proposed. Among these solutions, most recent schemes use Expansion Embedding (EE) modulation [3][4], Histogram Shifting(HS) [5] and dynamic predictive error histogram shifting (DPEHS)[6] modulation or, more recently, their combination. One of the main concern with these modulations is to avoid under-flows and over flows. The proposed reversible watermarking techniques [7][8] increases performance significantly.

This paper is organized in following sections. Section 2 reviews the related work. Section 3 gives a detail explanation of proposed work and algorithm. Section 4 gives expected results. Section 5 gives Conclusion. Followed by references.

II. RELATED WORK

Coatrieux and Guillou [1] proposed a new way to share and enhance medical image functionalities. While watermarking allows the sharing of information independently from the image format, the proposed knowledge digest gives a synthetic description of the image content, a digest that can be used for retrieving similar images with either the same findings or differential diagnoses. To provide updates for distant user similarity rules, and case and knowledge databases KD combined with watermarking appears to be a flexible solution.

Coatrieux et al. [2] focuses on the complementary role of watermarking with respect to medical information security (integrity, authenticity) and management. Reviewed sample cases where watermarking has been deployed. He concluded
that watermarking has found an important role in healthcare systems, as an instrument for protection of medical information, for secure sharing and handling of medical images.

Tian et al. [3] presented a simple and efficient reversible date-embedding method for digital images. Reversible data embedding has drawn lots of interest recently. Being reversible, the original digital content can be completely restored. In this paper, he presented a novel reversible data embedding method for digital images. The redundancy in the digital content to achieve reversibility was explored. Both the payload capacity limit and the visual quality of embedded images are among the best in the literature.

Thodi and Rodriquez [4] presented the histogram-shifting technique to remedy the two major drawbacks of Tians algorithm: the lack of capacity control and undesirable distortion at low embedding capacities. This then described two new reversible watermarking algorithms, combining histogram shifting and difference expansion: the first one using a highly compressible over own map and the second one using flag bits. A new, reversible, data-embedding technique called prediction-error expansion was then introduced and

watermarking algorithms based on the prediction- error expansion technique were presented.

Ansari, and Wei [5] Proposed a novel robust lossless data hiding technique, which does not generate salt-and-pepper noise. By identifying a robust statistical quantity based on the patchwork theory and employing it to embed data, differentiating the bit-embedding process based on the pixel groups distribution characteristics, and using error correction codes and permutation scheme, this technique has achieved both losslessness and robustness. It has been successfully applied to many images, thus demonstrating its generality. The experimental results show that the high visual quality of stego-images, the data embedding capacity, and the robustness of the proposed lossless data hiding scheme against compression are acceptable for many applications, including semi-fragile image authentication. Specifically, it has been successfully applied to authenticate losslessly compressed JPEG2000 images, followed by possible transcoding. It is expected that this new robust lossless data hiding algorithm can be readily applied in the medical field, law enforcement, remote sensing and other areas, where the recovery of original images is desired. Proposed a novel robust lossless image data hiding scheme, which employs a robust statistical quantity to mitigate the effect of image compression and small incidental alteration for data embedding.

Sachnev and Kim [6] present a reversible or lossless watermarking algorithm for images without using a location map in most cases. This algorithm employs prediction errors to embed data into an image. A sorting technique is used to record the prediction errors based on magnitude of its local variance. Using sorted prediction errors and, if needed, though rarely, a reduced size location map allows us to embed more data into the image with less distortion. The performance of the proposed reversible water- marking scheme is evaluated using different images and compared with four methods: those
of Kamstra and Heijmans, Thodi and Rodriguez, and Lee et al. The results clearly indicate that the proposed scheme can embed more data with less distortion.

Kamstra et al. [7] proposed a high-capacity lossless data-embedding methods are investigated that allow one to embed large amounts of data into digital images (or video) in such a way that the original image can be reconstructed from the watermarked image. He presented two new techniques: one based on least significant bit prediction and Sweldens lifting scheme and another that is an improvement of Tians technique of difference expansion. The new techniques are then compared with various existing embedding methods by looking at capacity distortion behavior and capacity control.

III.PROPOSED WORK

A. Objective

The proposed technique should protect images consisting of sensitive contents and should be able to extract the watermark with less distortion. It has following objectives:

- Should insert more data with lower distortion than any existing schemes.
- Improve PSNR
- Provide security to images
- Withstand Attacks

B. Methodology

When an input image is given, then the histogram shifting method is utilized to shift histogram to create gap for embedding watermark and visual cryptography is used to encrypt the watermark. Embedding and Extraction are two important steps for Watermarking. By shifting histogram we can embed secret data into host image. In the embedding phase, a binary matrix is created from the host image and a secret key. This

binary matrix, along with the secret binary image (watermark), generates a Master Share according to the predefined encryption rules of the VC Scheme. The Master Share has to be registered with a trusted third party for further verification. The watermarked image is usually transmitted or stored. If a person makes a modification to the marked image, it is called an attack. While resolving the rightful ownership, the same secret key is used to generate the Verification Share. Then the Verification Share and the MasterShare (kept by the trusted third party) are combined to recover the hidden watermark Histogram Shifting and visual cryptography [9] are explained below.

1. Histogram Shifting

The basic principle of Histogram Shifting modulation, illustrated in Fig 1. in a general case, consists of shifting a range of the histogram with a fixed magnitude , in order to create a gap near the histogram maxima (C_1 in Fig.1). Pixels, or more generally samples with values associated to the class of the histogram maxima (C_0 in Fig. 1(b)), are then shifted to the gap or kept unchanged to encode one bit of the message, i.e., 0 or 1. Samples that belong to this class named as carriers. Other samples, i.e., noncarriers, are simply shifted. This message is encrypted using visual cryptography for more security. At the extraction stage, the extractor just has to interpret the message from the samples of the classes C_0 and $C_1$and invert watermark distortions (i.e., shifting back shifted value).In order to restore exactly the original data, the watermark extractor needs to be informed of the positions of
samples that have been shifted out of the dynamic range (V_{Min} and V_{max} Fig. 1 (b)).This requires the embedding of an overhead and reduces the watermark capacity. HS will provide good performances within black areas in medical images where the pixels have all most null gray values .

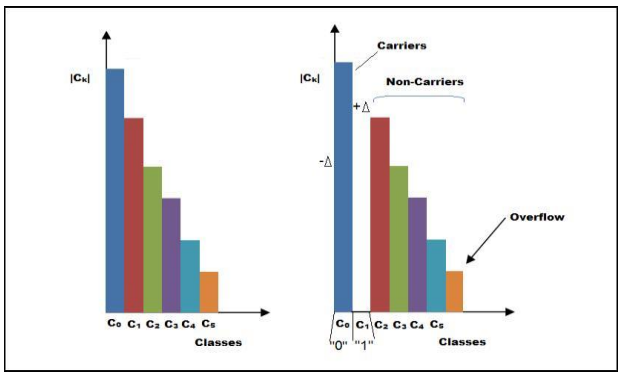

Fig 1. Histogram shifting modulation. (a) Original histogram. (b) Histogram of the watermarked data.

The given algorithm [5] is used to find maximum and minimum point in histogram. The objective of finding the peak point is to increase the embedding capacity as large as possible since in this algorithm, as shown below, the number of bits that can be embedded into an image equals to the number of pixels which are associated with the peak point. Pseudocode Embedding Algorithm with one pair of Maximum and Minimum Points is considered. For an M×N image, the range of each pixel is of grayscale value x ε [0,255].

1) Generate histogram H(x) of the original image.

2) In the histogram H(x), find the maximum point h(a), where a ε [0,255] and the minimum point zero h(b), where b ε [0,255]

3) If the minimum point h(b)>0, recode the coordinate (i,j) of those pixels and the pixel grayscale value b is taken as overhead. Then set h(b)=0

4) Without loss of generality, assume a<b. Move the whole part of the histogram H(x) with x ε (a,b) to the right by 1 unit.
This means that all the pixel grayscale values are added by 1

5) Scan the image, once check the pixel (whose grayscale value is a). Check the bit to be embedded. If the to be embedded bit is"1", then the pixel grayscale value is changed to a+1. If the bit is"0", then the pixel value remains a.

6) Apply visual cryptography to the secret data before embedding.

If the required payload is greater than the actual capacity, more pairs of maximum point and minimum point need to be used.

2. *Visual Cryptography*

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used.. It is best-known techniques proposed by Moni Naor and Adi Shamir, To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Table 1 illustrates the scheme of encoding one pixel in a (2, 2) VC scheme. A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary blocks of sub-pixels. While creating the shares, if the given pixel p in the original image is white, then the encoder randomly chooses one of the first two columns of Table 1. If the given pixel p is black, then the encoder randomly chooses one of the last two columns of Table 1. Each block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. Thus no information is gained by looking at any group of pixels on a share, either.

Pixel	White		Black	
Prob.	50%	50%	50%	50%
Share1				
Share2				
Stack Share1&2				

Table 1.A (2, 2) Visual Cryptography Schem

3. Embedding:

The host image in which secret data is to be embedded is first partitioned. The secret data to be embedded is encrypted using visual cryptography. so we get transparencies and this image is then embedded in host image by using histogram shifting method. Hence we get watermarked image. This scheme assumes that the binary secret data (watermark) S of size *wxh* is to be embedded into the host image H of size rxc.Let K be a random integer selected by the owner as a secret key. The output of the embedding phase is a watermarked image O of size *rxc*(same as the original host image) and a Master Share M of size *wx2h.*

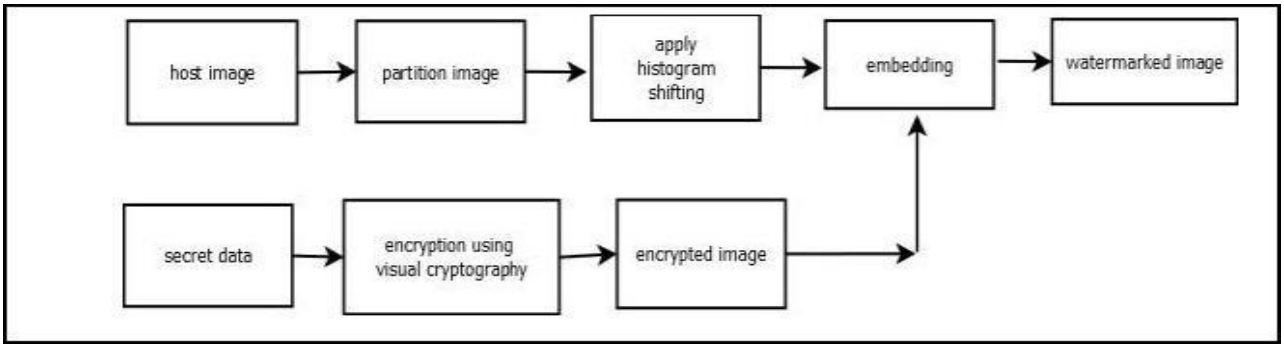

Fig 2. Embedding

Inputs: A Host Image H, a Binary Watermark S, and a Secret Key K

Outputs: Marked Image O and a Master Share M
The watermark embedding procedure is as follows:

Step1: The secret key K is used as a seed to generate *Wxh* random numbers over the interval [1 to *rxc*]. Let R_i be the i^{th} random number.

Step2: Creation of a binary matrix X of size *wxh* such that the entries in the array are the most significant bits of R_i^{th} pixel of the host image.

Step3: Creation of a binary matrix Z of size *wxh* such that the entries in the array are the most significant bits of the R_i^{th} random number.

Step4: Creation of a binary matrix Y of size *wxh* such that
Yi= XOR (Xi , Zi)

Step5: Creation of a Master Share M by assigning a pair of bits for each element in the binary matrix Y according to the predefined encryption rules of VC as shown in Table 2. Finally, the Master Share is registered with a trusted third party.

Color of i^{th} pixel in binary watermark(S_i)	i^{th} entry in binary array(Y_i)	Pair of bits to be assigned in master share
Black	1	(0, 1)
Black	0	(1, 0)
White	1	(1, 0)
White	0	(0, 1)

Table 2.Encryption Rules to Create Master Share

3. *Extraction*

In extraction stage histogram shifting is used for extracting encrypted image. After extraction we get encrypted image which is then decrypted using visual cryptography to get secret data.

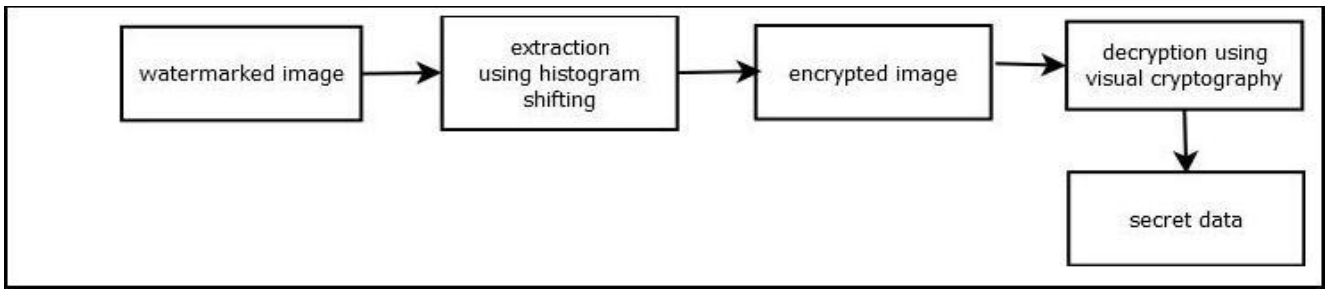

Fig 3. Extraction

Detection (also called extraction) is an algorithm which is applied to the attacked image to extract the watermark from it. In robust (secure) watermarking applications, the extraction algorithm should be able to reproduce the watermark, even if the modifications were strong.
Inputs: Modified image O', Master Share M, and a Secret Key K
Output: Extracted Watermark S'

The watermark detection procedure is as follows:

Step1: The secret key K is used as a seed to generate wxh random numbers over the interval *[1 to rxc]*. Let Ri be the i^{th} random number.

Step2: Creation of a binary matrix X of size *wxh* such that the entries in the array are the most significant bits of Ri^{th} pixel of the host image.

Step3: Creation of a binary matrix Z of size *wxh* such that the entries in the array are the most significant bits of the Ri^{th} random number.

Step4: Creation of a binary matrix Y of size *Wxh* such that *Yi= XOR (Xi ,Zi)*

Step5: Creation of a Verification Share such that, if the element in the binary matrix Y is '0' then Vi = (0, 1) has to be assigned,else Vi= (1, 0) has to be assigned.

Step6: The secret image can be extracted by performing logical OR operation as follows: *Si' = OR (Mi , Vi).*

D. *Advantages of Proposed System*

- Directly applying HS on pixels may be more efficient and of smaller complexity than applying it on prediction-errors.
- The watermark embedder and extractor remain synchronized because the extractor will retrieve the same reference image. This process is adaptable to select the most locally appropriate watermarking modulation.
- Visual Cryptography, when used in copyright protection enables resolution of rightful ownership, without using the original image. Also, the host image will not be altered during the embedding process.

IV. RESULTS

The result is shown in this section this implementation provides various modes of visual cryptography applied and provision for overlaying transparencies. After overlay the result is displayed. In practice, there is a very good chance for the watermarked image to be altered (intentionally and unintentionally) while being transmitted through the channel. These alterations may be a result of intentional attacks such as filtering, blurring, etc. or unintentional distortions such as JPEG compression, channel noise addition etc. To test the robustness of the proposed algorithm, the watermarked images were subjected to various image manipulating operations and compression attacks. All attacks are implemented using the java swing. Finally, the performance of the algorithm with respect to attack resilience has been established shown in Fig 5, Experimental results reveal that the watermark pattern is well recognizable, even after making severe modifications to the marked image. As long as the extracted watermark is recognizable, the purpose is served.

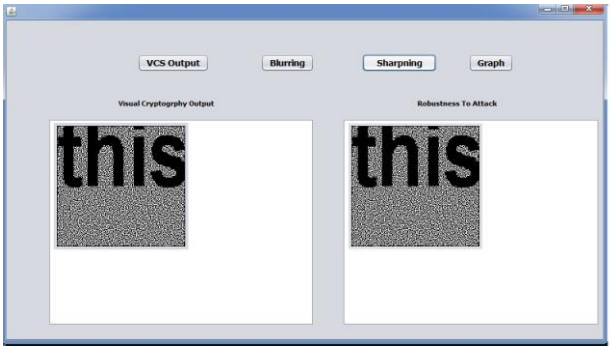

Figure 5:output of sharpening Attack

V. CONCLUSION

The proposed reversible watermarking scheme combines two distinct modulations, pixel histogram shifting and Visual cryptography. This watermarking scheme offers better security, so that, attackers will not be able to detect ownership information Visual cryptography has the ability to restore a secret image without the use of computation. It also provides security to the embedded data and withstand attacks or modifications. One of the major upcoming challenges is about the robustness of the watermark which can be implemented in future.

ACKNOWLEDGEMENT

I would like to take this opportunity to acknowledge the contribution of certain people without which it would not have been possible to complete this paper work. I am thankful to the Principal Dr. R. K. Jain, Guide, Head, Coordinators, Colleagues of the Department of Computer Engineering, Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune, Maharashtra, India, for their support, encouragement and suggestions. I would like to express my special appreciation and thanks to my guide Professor Dr. Reena Gunjan, who has been a tremendous mentor for me.

REFERENCES

[1] **G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux**, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 158–165, Mar. 2009.

[2] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A review of image watermarking applications in healthcare," in Proc. IEEE EMBC Conf., New York, 2006, pp. 4691–4694.

[3] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[4] D.M. Thodi and J. J. Rodriquez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007

[5] Z. Ni, Y. Q. Shi, N. Ansari, and S.Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[6] V. Lavanya, G. Annapoorani" Dynamic Histogram Shifting for Reducing Distortion in Image Embedding „International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2014

[7] Sachnev,H.J.Kim,J.Nam,S.Suresh,andY.Q.Shi,"Reversible-watermarking algorithm using sorting and prediction,"IEEE Trans. Circuit Syst.Video

Technol. , vol. 19, no. 7, pp. 989–999, Jul. 2009.

[8] H. J. Hwang, H. J. Kim, V. Sachnev, and S. H. Joo, "Reversible watermarking method using optimal histogram pair shifting based on pre- diction and sorting," KSII, Trans. Internet Inform. Syst.,vol.4,no.4, pp. 655–670, Aug. 2010

[9] B Surekha , Dr GN Swamy , Dr K Srinivasa Rao , A Ravi Kumar "A Watermarking Technique based on Visual Cryptography " Journal Information Assurance and Security 4 (2009) 470-473

