Digital Watermarking Based on Visual Cryptography and Histogram

R. Rama Kishore, Sunesh

Abstract—Nowadays, robust and secure watermarking algorithm and its optimization have been need of the hour. A watermarking algorithm is presented to achieve the copy right protection of the owner based on visual cryptography, histogram shape property and entropy. In this, both host image and watermark are preprocessed. Host image is preprocessed by using Butterworth filter, and watermark is with visual cryptography. Applying visual cryptography on water mark generates two shares. One share is used for embedding the watermark, and the other one is used for solving any dispute with the aid of trusted authority. Usage of histogram shape makes the process more robust against geometric and signal processing attacks. The combination of visual cryptography, Butterworth filter, histogram, and entropy can make the algorithm more robust, imperceptible, and copy right protection of the owner.

Keywords—Butterworth filter, digital watermarking, histogram, visual cryptography.

I. Introduction

In today's era, technology is growing in a greater pace but it can cut both ways in terms of fast transmission and manipulation. Resultantly, Security concern over copyright protection of digital media objects has become a challenging issue. Watermarking comes out as a raising solution to tackle this problem. Digital watermarking is a technique in which pattern of bits are embedded into digital media object. Watermarking can be applied to various multimedia objects like audio, video and image [2]. In this paper, emphasis is done on digital image watermarking. The method of watermarking is appreciated based on its characteristics for achieving copyright of owner are robustness, imperceptibility, capacity, security, unambiguity, and blindness [1], [6].

Robustness basically refers the capability of extracting correct watermark after yielding the attacks [1], [2]. Imperceptibility connotes that watermark should be self-effacing [1]. Unambiguity specifies that extracted watermark should be precisely verifying the copyright of owner [6]. Blindness implies that original media objects are not required in extraction process of watermark [6]. Security cites to the shield against illegal watermark extraction [6].

For achieving conditions stated above, various watermarking algorithms have been reported in literature. Many of these are robust but they do not cope well with other conditions. To preserve the security of secret image, Naor and Shamir in 1994 proposed a scheme named visual secret sharing scheme VSS or visual cryptography (VC) [12], [14]. The main aid of visual cryptography is that it does not modify the secret image and decryption is performed by human visual system [14]. Visual cryptography scheme divides secret image into various random looking shares. Consider (2, 2) VC scheme which divides secret image into two shares. This VC scheme allows freely distributing one of the shares, and second share can be used as key which required reconstructing the secret image. It is feasible to hide one share from others in order to protect secret image. So, it means that the hidden share can be used as a key for decryption of the original image. With this viewpoint, VC has been considered to attain the protection of watermark in combined scheme, whereas key share is required to reconstruct embedded watermark. In this way, this scheme can be used to resolve any dispute of image ownership and accomplish copy right of owner [12].

In this paper, (2, 2) visual cryptography is combined with the histogram shape based watermarking. The adoption of visual cryptography with watermarking helps in achieving characteristics of copyright of an owner.

To achieve robustness to signal processing and geometric attacks, Butterworth filtering and histogram shape property has been taken into account. In order to increase security and robustness, both watermark and host data are preprocessed before embedding process. Then watermark is embedded by maintaining histogram shape property. The histogram shape property for embedding watermark will be discussed in coming section.

The organization of this paper is as follows. Section II provides a short review on digital watermarking based on histogram shape and visual cryptography methods. Section III illustrates proposed embedding method and section IV states proposed decoding method. Finally, section V concludes this paper.

II. Related Work

In this section, the concepts of visual cryptography and watermarking techniques are reviewed. Firstly, watermarking scheme based on histogram is illustrated. Afterwards, visual cryptography is discussed.

A. Watermarking Scheme Based on Histogram

In literature, many watermarking methods which utilized concept of histogram and low pass filtering are reported. Most watermarking techniques presented which use the statistical concept of image histogram.

Dr R.Rama Kishore is Associate Professor, University school of Information and Communication Technology, G.G.S.Indra prastha University, Delhi, India (e-mail : ram_kish@yahoo.com).

Ms Sunesh is Assistant Professor, MSIT, Delhi. Research Scholar at G.G.S.Indra prastha University, Delhi, India (e-mail: suneshmlk@gmail.com).

Histogram is an emphatic tool to represent pixel distribution of an image. Image histogram yields the summary of intensities of image but it is unable to cite any information related to the spatial relationship between pixels [3]. Property of histogram shape is used here to achieve robustness against geometric attacks as it is independent of pixel position. Image histogram is a statistical concept [2]-[5].

Suppose that gray scale image I is size of M*N having 8-bit depth. In 8-bit gray scale image, there are 256 gray levels from 0 to 255. So, histogram H of an image I in [2] can be represented as:

$$H = \{h(j)|j = 0,1 \dots\dots 255\} \tag{1}$$

where h(j) is number of pixels whose pixel value is j in an image I. and

$$M.N = \sum_{j=0}^{255} h(j) \tag{2}$$

Here, M and N shows the number of rows and columns in the image I.

Tianrui et al. [1] proposed robust histogram shape-based method in which histogram shape related index and high frequency component modification HFCM scheme is utilized to achieve robustness against signal processing and geometric attacks. The use of HFCM compensates the side effects of Gaussian filtering and also improves robustness.

Tianrui et al. [2] reported a histogram shape based robust image watermarking scheme. This scheme is robust to cropping and random bending attack. Embedding process completely depends on histogram shape which provides robustness. In this paper, author first extracted low frequency component and then embeds watermark by using the histogram shape property.

Kiran et al. in [3], [4], utilized Butterworth filter for extracting low frequency component and histogram shape property for embedding watermark. However, watermark embedding is done by bin shifting within group by maintaining the histogram shape.

Xuansen et al. [5] presented a resistant image watermarking method against geometric attack for the gray images. Watermark has been embedded into cover image by modifying number of samples of three consecutive bins and only one bin of two adjacent bins is modified every time. In this scheme repetition of same bin modification is avoided. This scheme is robust but may not resist a key estimation attack. Scheme requires security to be increased.

In the study of Shijun et al. [7], robustness of hash function is achieved by using low pass filter and using histogram invariance property. Implementation of Hash function used in this as hash sequence is extracted from the histogram of low frequency component at spatial domain.

Xuefeng et al. [8] reported a watermarking scheme based on histogram modificationin which visual quality of watermarked image is considered. This scheme is robust to geometric distortions and image processing attacks. Shumei et al. [9] presented robust watermarking approach based on histogram which preserves visual quality of watermarked images.

Hamidreza et al. [10] developed a novel watermark decoder in contourlet domain and by utilizing inverse Gaussian distribution which is highly robust.

J. Veerappan et al. [11] proposed a geometric attack resistant image watermarking scheme for providing high security. In this, security is ensured by AES technique.

The watermarking schemes explained in [1],[2],[3],[4] employs low pass filters to extract the low frequency component so that watermark can be embedded into the low frequency component only. This constructs the scheme to resist against signal processing attacks.

B. Visual Cryptography

Visual cryptography has been exploited in various fields to preserve security. With this perspective visual cryptography is employed in watermarking. Visual cryptography permits encoding of secret image. The concept of visual cryptography is shown in Fig. 1

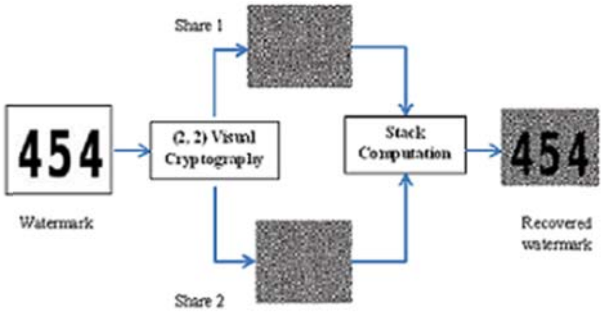

Fig. 1 Concept of Visual Cryptography [6]

According to the concept of visual cryptography, each pixel of secret image is replaced by sub pixels. A secret image with P by Q pixels can be dividing into two shares with 2P by 2Q pixels. At decryption side, secret image is recovered by stacking the two shares. Each pixel may be replaced by two sub pixels or four sub pixels as shown Figs. 2 and 3.

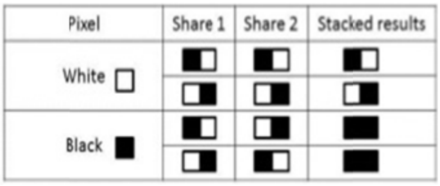

Fig. 2 Basic (2, 2) VC scheme two sub pixels [13]

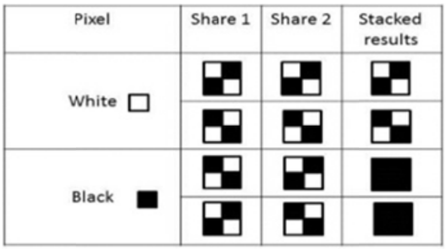

Fig. 3 Basic (2, 2) VC scheme with four sub pixels [13]

In last few years, various watermarking techniques have been associated with VC [6], [12]-[14], [19], [21]-[28]. One of the first attempts to use VC in watermarking has been presented in [19]. In this, embedding took place into two phases. At the first step, watermark is divided into two random noise looking shares. In second phase, one share of watermark which is called as cipher is embedded into host data, and the result is called stego image. If One of these two shares is modified, then watermark cannot be revealed.

Han Yan-yan et al. [15] reported (2, 2) visual cryptography scheme in addition to traditional cryptography. Jithi et al. [16] developed a progressive visual cryptography for meaningful shares. The formation of meaningful shares has accomplished by combining watermarking with visual cryptography. At decryption, secret image is published gradually by superimposing more and more shares progressively. Ming et al. [17] reported Joint Visual cryptography and watermarking method in history. Firstly, noise is injected into host image. Afterwards, pair conjugates error diffusion is performed for generation of shares. Noise aids in diverting hacker's attention from the shares. W.P. Fang et al. [18] presented a progressive viewing scheme for sharing of sensitive images where each pixel is expanded into 2*2 block B(x, y).

In [12], [13], [20], depending upon type of VC employed with watermarking, classification of digital watermarking based on VC is carried out into three different types. First one is watermarking using (2, 2) VC. Second one is watermarking using (2, n) VC, and the last one is watermarking using (k, n) VC.

(2, 2) VC is employed for achieving copyright protection of images in [6], [22], [24]. In [6], scheme employs characteristics of DWT while in [22] DWT and SVD is adopted.

Robust scheme has been proposed based on Fractional Fourier transform, SVD, and VC that helps in enhancing robustness and security by Sanjay et al. [14]. In [23], [25], [26], multiple watermarks are inserted. Scheme presented in [27] is blind, invisible, and robust. In this, image is preprocessed by using DT-DWT and shares are generated using pixel expansion. For security of medical digital content, Medical image watermarking scheme has been proposed in [21] that adopts DT-CWT with (2, 2) Visual Cryptography.

Rawan et al. [28] reported a HSV image watermarking scheme based on VC. In this method, first features are extracted from histogram of H, S, and V planes of HSV image. Afterwards embedding is done by using VC.

III. Proposed Embedding Method

In this paper, a method is proposed to maintain security and robustness. (2, 2) VC and histogram shape property is exploited in watermark embedding and decoding. At embedding, watermark and cover image both are preprocessed first. On watermark, VC is applied to ensure copyright of owner and cover image is processed by enforcing Butterworth low pass filter on it. Use of the Butterworth filter enhances robustness to signal processing attacks. Then, filtered image is utilized for embedding the watermark share.

Watermark embedding mainly contains two parts; the first one is called preprocess, and the other one is watermark share embedding. Watermark embedding is shown by block diagram of watermark embedding process in Fig. 4.

A. Preprocess

In preprocess host image and watermark both are processed. Watermark is processed by applying VC, and host image is processed by using Butterworth filter.

1) VC: Apply (2, 2) VC on watermark. As a resultant, it generates two shares called W1 and W2. Share W1 will be inserted into cover image I, and share W2 is submitted to trusted authority for achieving copyright of owner. Encoding of watermark by means of shares makes scheme secure and robust.
2) Butterworth Filter: Employ Butterworth filter on the cover image I for extracting low frequency component I_{Low}. Robustness to common signal processing attacks may be attained by embedding watermark into low frequency component.

B. Watermark Share Embedding

Watermark share is embedded into low frequency component of cover image by utilizing histogram shape property. Watermark share embedding process is further subdivided into four steps as explained below:

1) Histogram Construction: Generate histogram of extracted low frequency component I_{low} of Cover Image.

$$H_{low}(j)=h_{low}(j) \text{ and } j = 0,1\ldots\ldots,255 \tag{3}$$

where $h_{low}(j)$ denotes number of pixels of intensity value j.

2) Embedding Range Selection: In this, location is selected for inserting watermark. Here, output of previous steps becomes input i.e. use extracted histogram $h_{low}$of $I_{low.}$

First, combine two gray level as a bin BI expressed as:

$$BI(j) =h_{low}(2*j)+h_{low}(2*j+1) \tag{4}$$

and then combine two neighboring bins as group written below [1]-[4]:

$$G(j) = BI(2*j) + BI(2*j +1) \tag{5}$$

Number of pixels in j^{th}group is N_{gj}.

Range for embedding is depends on N_{gj} and threshold T_a.

```
IF($N_{gj}$>= $T_a$) Then
select $N_{gj}$ for embedding.
ELSE
Drop $j^{th}$ group for embedding.
END                                                    (6)
```

Apply this procedure for all groups in G. and find all eligible groups for embedding [1]-[4]. These eligible groups are denoted by E. and length of watermark is notated as L. whereas in this length of watermark should be less than E. so choose N groups with most pixels for embedding. Selection of groups among the eligible groups can be further optimized by taking entropy in to consideration.

3) Embedding of Watermark: Ensuing the embedding range selection, each selected group will be used for carrying watermark bit. Processed watermark called watermark share W1 is used for embedding. Watermark share W1 is embedded into selected groups of low frequency components of image by maintaining histogram shape and produces output called ${}^{W}I_{low.}$ Watermark share W1 is represented as [2], [4]

$$W1=\{w(i) \mid i=0,1,\ldots..L) \tag{7}$$

The embedding criteria for the watermark bits are as [4]:

$$IF(W1(i)=1\ ) \text{ then } BI1/BI2>=T_a \tag{8}$$

$$IF(W1(i)=0\ ) \text{ then } BI2/BI1>=T_a \tag{9}$$

4) Generation of Watermarked Image: Combine high frequency component of cover image I high with watermarked low frequency component $^{\mathbf{W}}\mathbf{I}_{\mathbf{low.}}$ Finally produces watermarked image WI.

$$WI = {}^{\mathbf{W}}\mathbf{I}_{\mathbf{low}}+\mathbf{I}_{high.} \tag{10}$$

This completes process of embedding watermark and also represented by block diagram. This diagram explains process of embedding watermark into cover image I. Robustness is controlled by defining bin size and embedding range. But if number of pixels in a group may be modified by attackers. In order to tackle this problem, safe band are used between watermarked and non-watermarked groups.

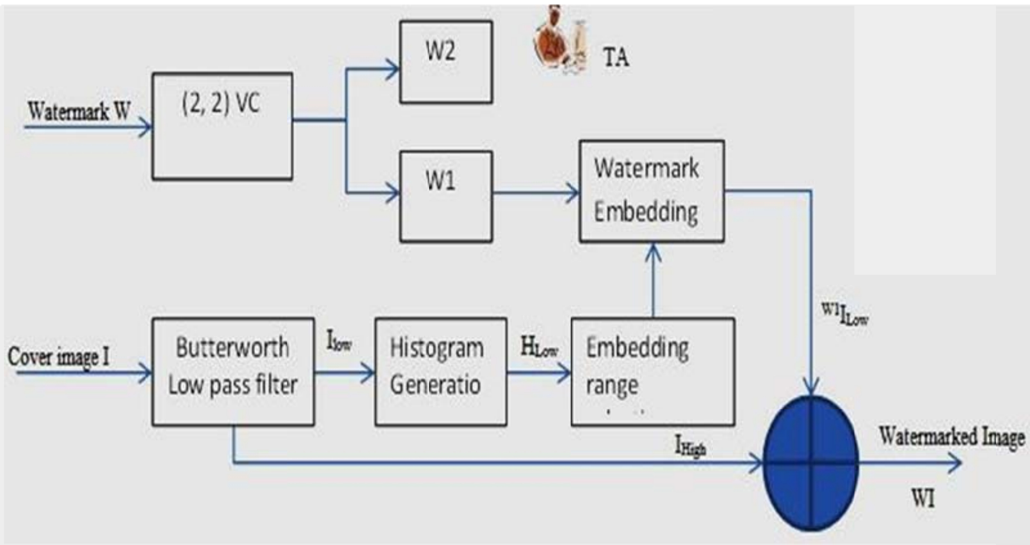

Fig. 4 Block Diagram of Proposed Embedding Process [4]

IV. Proposed Decoding Method

At decoding, first watermarked range is obtained, and then watermark share is extracted. The original watermark is revealed only by stacking extracted share and key share. Fig. 5 shows proposed extraction process.

Extraction process takes watermarked image as an input. This process follows same steps as in embedding process. By using this procedure only one watermark share W1 is extracted. For original watermark W, watermark share W2 is required which is preserved by trusted authority. Original watermark W is attained by applying VC. When both watermark share W1 and W2 are stacked together then original watermark is revealed. Detailed process of watermark decoding is stated below:

Input: Watermarked Image WI.
Output: Watermark W
Step 1. Read watermarked image file WI.
Step 2. Employ Butterworth low pass filter to extract low frequency component of watermarked image $WI_{low..}$
Step 3. Generate histogram of detected low frequency component of watermarked image

$WH_{low}(j)=Wh_{low}(j)$ and $j = 0,1\ldots\ldots,255$

where j denotes number of pixels of intensity value j.

Divide the histogram bins as groups, each group consist of two adjacent bins (bin1 and bin2) and their population is BI1` and BI2` respectively.

Step 4. Select N groups with most number of pixels as watermarked groups.
Step 5. By computing the ratio between BI1` and BI2` of each group, one inserted bit is extracted in reference to,

W1(i) = 1, if BI1`/ BI2` ≥ 1
W1(i) = 0, otherwise.

The process is repeated until all bits are extracted.

Step 6. Extracted watermark share is depicted as W1= `(i)| i=0,1,2……. L All L bits are extracted.

Step 7. Step 7: Extracted watermark share W1 is combined together with watermark share W2 to reconstruct original watermark.

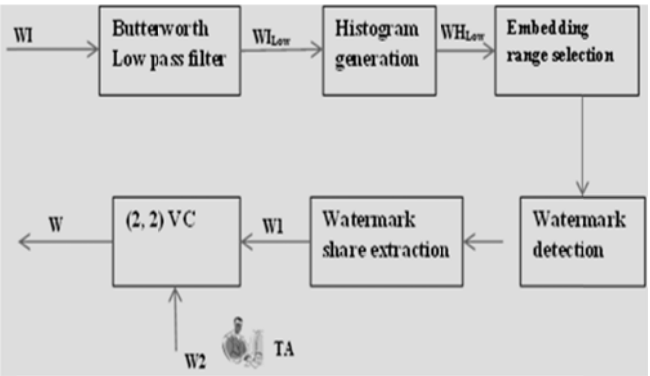
WI
Butterworth Low pass filter
WI_Low
Histogram generation
WH_Low
Embedding range selection
Watermark detection
Watermark share extraction
W1
(2, 2) VC
W
W2
TA

Fig. 5 Block Diagram of Proposed Extraction Process [4]

V. Conclusion

This paper proposes a method on robust image watermarking scheme for achieving the copyright protection of owner. This method combines Butterworth filter, histogram shape, and (2, 2) VC schemes together. In this, some of the benefits from this proposed method would be as follows:

1. Work related to VC, histogram and Butterworth is reviewed and suggested a new method aiming more imperceptibility, robustness and copyright protection of owner.
2. Combining VC, histogram, entropy and Butterworth filter improves the watermarking scheme compared to applying them individually.
3. For ensuring security and robustness in the proposed method, watermark and host image is pre-processed by VC and Butterworth worth filter.
4. Watermark cannot be retrieved from other similar image.
5. Use of Butterworth low pass filter and entropy will make the scheme imperceptible and resistant against signal processing attacks as it extracts low frequency component of cover image such that watermark will only be embedded into low frequency component.
6. (2, 2) VC generates two shares of watermark called W1 and W2 which enhance robustness, security and also provide copyright protection of owner.
7. Histogram shape property is taken into account for embedding watermark share into host image. As, the histogram shape property is independent to the pixel location. Mathematically, it is invariant to the scaling and that will resist against geometric attack.

References

[1] Tianrui Zong, Young Xiang, Iynkaran Natgunanathan, Song Guo, Wanlei Zhou and Gleb Beliakov, “Robust Histogram Shape-Based Method for Image Watermarking”, IEEE Transactions on circuit and system for Video Technology, Vol.25, No.5, pp.717-729, 2015.

[2] Tianrui Zong, Yong Xiang, and Iynkaran Natgunanathan, "Histogram Shape Based Robust Image Watermarking Method", IEEE ICC Communication and Information System Security Symposium, pp. 878-883, 2014.

[3] Kiran, Kawal Garg and Girdhar Gopal, “Robust Image Watermarking based on Histogram Shape and Butterworth Filtering”, International Journal for scientific Research & Development (IJSRD), Vol. 3, Issue 03, pp.2581-2584, 2015.

[4] Kiran and Kawal Garg. “Watermark Embedding and Extraction using Histogram Shifting and Butterworth Filtering”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 5, pp. 1481-1487, 2015

[5] Xuansen He, Tao Zhu, and Gaobo Yang, "A geometrical attack resistant image watermarking algorithm based on histogram modification", Springer, pp. 291-306, 2013.

[6] Der-Chyuan Lou, Hao-Kuan Tso and Jiang-Lung Liu, "A Copyright Protection Scheme for Digital Images Using Visual Cryptography Technique", Computer Standards & Interfaces Elsevier, Vol 29, pp. 125-131, 2007.

[7] Shijun Xiang, Hyoung Joong Kim and Jiwu Huang, “Histogram-Based Image Hashing Scheme Robust Against Geometric Deformations”, In Proceedings of the 9th workshop on Multimedia & security, pp. 121-128. ACM, 2007

[8] Xuefeng hu and Daoshun Wang et al, “A histogram based watermarking algorithm robust to geometric distortions,” in Proc. ICECEE, pp. 773-779, 2015.

[9] Shumai Wang, Wenbao Hou, “A robust watermarking algorithm based on histogram,’’ in Proc. IWISA 2009, pp. 453-456,2009.

[10] Hamidreza Sadreazami, M. Omair Ahmad and M.N.S Swamy, “Multiplicative Watermark Decoder in Countourlet domain using normal inverse Gaussian distribution,” IEEE Transactions on Multimedia vol.18, no.2, Feb2016.

[11] J. Veerappan and G. Pitchammal, “Geometric Attack Resistant Multilayer Image Watermarking Scheme for Providing High Security”, arXiv preprint arXiv:1210.5941,2012

[12] James Ching-Nung Yang, and Chih-Cheng Wu Stelvio Climato, "Visual Cryptography based watermarking: Definition and Meaning," Springer, 2013.

[13] Stelvio Cimato, James C.N. Yang and Chih -Cheng Wu, "Vsual Cryptography based watermarking," In Transactions of data hiding and Multimedia Security IX, pp. 91-109, 2014.

[14] Sanjay Rawat, Balasubramanian Raman, "A blind Watermarking Algorithm based on fractional Fourier transform and visual cryptography," Signal Processing 92, no. 6, pp. 1480-1491, 2012.

[15] Han Yan-yan, Xián China, "A watermarking-based Visual Cryptograhy scheme with meaningful shares," in IEEE International Conference on computational Intelligence and security, 2011, pp. 870-873.

[16] Jithi PV, Anitha T Nair, "Progressive Visual Cryptography with watermarking for meaningful shares," in International Multi-Conference on Automation, Computing, Communication, Control and compressed sensing, 2013, pp. 394-401.

[17] Oscar C. Au. Ming Sun Fu, "Joint Visual Cryptography and Watermarking," in IEEE International Conference on Multimedia and Expo, 2004, pp. 975-978.

[18] J. C. Lin, W. P. Fang and, "Progressive Viewing and sharing of sensitive images," Pattern recognition and Image analysis, vol. 16, no. 4, pp. 632-636, 2006.

[19] Pei-Min-Chen Young-Chang-Hou, "An asymmetric watermarking scheme based on visual cryptography," in ICSP, 2000.

[20] Sunesh, R. Rama Kishore,” Digital watermarking based on visual cryptography”, in Vth International Symposium on fusion of Science and Technology, New Delhi, pp. 279-285,2016.

[21] Meryem Benyoussef, Samira Mabtoul, Mohamed EI Marraki, Driss Aboutajdine, "Medical Image watermarking for copyright Protection based on Visual Cryptography," in IEEE ICMCS, 2014, pp. 93-98.

[22] Abusitta, Adel Hammad, "A Visual Cryptography Based Digital Image Copyright Protection," Journal of Information Security (Scientific Research), pp. 96-104, April 2012.

[23] Mathivadhani, C. Meena, "Digital watermarking and information hiding using wavelets, SLSB and Visual cryptography method," in IEEE International Conference on Computational Intelligence and computing Research, 2010.

[24] Tzung-Her chen and Du-shiau Tsai, "Owner-Customer copyright protection mechanism using a watermarking scheme and a watermarking protocol," The Journal of Pattern Recognition society, pp. 1530-1541, 2006.

[25] Huo Luo, Zhe-Ming Lu and Jeng-Shyang Pan, "Multiple Watermarking in Visual Cryptography," Digital watermarking, pp. 60-70, 2008.

[26] Yanyan Han, Wencai He and Yixiao Shang, "DWT- domain Dual watermarking algorithm of color image based on visual cryptography," in IEEE 9th international Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013, pp. 373-378.

[27] Meryem Benyoussef, Samira Mabtoul, "Blind Invisible Watermarking Technique in DT-CWT domain using visual cryptography," Image Analysis and Processing, pp. 813-822, 2013.

[28] Rawan I. Zaghloul, Enas F. Al-Rawashdeh, "HSV image watermarking scheme based on visual cryptography", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:2, No:8, pp.2658-2661, 2008

R. Rama Kishore is currently working as an Associate Professor at University School of Information Technology and Communication Technology, G.G.S. Indraprastha University, Delhi. He received his PhD degree from G.G.S. Indra Prastaha University, Delhi and M. Tech from I.I.T. Delhi. His area of interests includes Computer Graphics, Multimedia technologies, Image processing etc.

Sunesh received B.E. degree in Computer Science and Engineering from Maharishi Dayanand University and the M.Tech degree from Chaudhary Devi Lal University, Haryana. She is currently an Assistant Professor with Maharaja Surajmal Institute of Technology, New Delhi, India and also working towards Ph.D. degree with University School of Information and Communication Technology, Guru Gobind Singh Indraprastha University, New Delhi, India.