© 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Watermarking and Cryptography Based Image Security Algorithms : A Survey

Amit Kumar Sharma, Aman Kumar
Department of Computer Science and Engineering, L.R. Institute of Engineering And Technology, Solan, Himachal Pradesh, India

ABSTRACT

With the coming era of Internet, more and more data are transmitted and exchanged on the networked systems to enjoy the rapid speed and convenience. However, in the cyberspace, the availability of duplication methods encourages the violation of intellectual property rights of digital data, such as document, image, audio, and video. Therefore, the protection of rightful ownership of digital data has become an important issue in recent years. This study discusses various algorithms developed over the years for securing digital images. Algorithms for watermarking (primarily based on transforms) and cryptography (primarily based on visual cryptography scheme) are discussed.

Keywords: Image Encryption, Cryptography, Watermarking, Survey

I. INTRODUCTION

With the recent advances in internet computing in our day to day life the need for communication has increased. Privacy in communication is desired when confidential information is shared between two parties. Without image security, we will end up giving our useful data to other people which may lead to some kind of loss. It is easy to transmit and duplicate, but unauthorized reproduction becomes a serious problem. It is, therefore, very important to have the capabilities to detect copyright violations and control access to digital media. Fueled by these concerns, data hiding has evolved as an enabler of potential applications for copyright protection such as access control of digital multimedia (e.g., watermarking), embedded captioning, secret communications (e.g., steganography), tamper detection, and others.

Data hiding is the art of hiding a message signal in a host signal without any perceptual distortion of the host signal. The composite signal is usually referred to as the stego signal. Data hiding is a form of subliminal communication. Any form of communication relies on a channel or medium. Data hiding, or steganographic, communications rely on the channel used to transmit the host content. As the stego content moves around the globe, perhaps over the Internet, or by any other means usually deployed for communicating the host signals, so does the embedded, covert message signal.

One of the most popular and powerful data hiding techniques is Steganography. It is the method of writing secret messages in such a way that no one apart from the sender and intended recipient even realizes about its existence. Steganography is the art and science of invisible communication which is accomplished through hiding information in other information, thus hiding the existence of the communicated information.

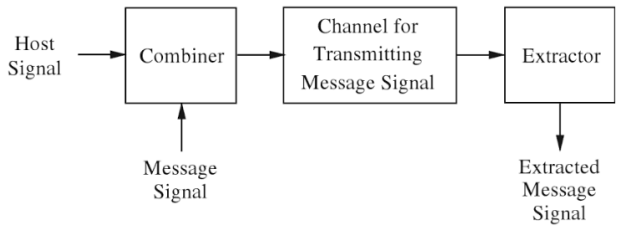


Figure 1: Communication by Data Hiding

Cryptography and watermarking are data hiding and data security techniques similar to steganography. Cryptography is the science of secret writing. In cryptography, cipher text is generated using a secret key over plain text, ciphering of text makes it unreadable, only the one who knows the secret key can decipher the message into plain text. The main objective of cryptography is to secure communications by changing the data into a form so that it cannot be understand by

an eavesdropper. 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.

A digital watermark is a signal which is permanently embedded into digital data that can be detected or extracted afterwards to confirm the authenticity of the data and the watermark may be hidden in the host data. Watermarking focuses on protecting the watermarked data or object so that it cannot be removed. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In watermarking applications like copyright protection and authentication, there is an active adversary that would attempt to remove, invalidate or forge watermarks. The watermark is hidden in the host data in such a way that it cannot be removed without demeaning the host medium. This work uses visual cryptography and watermarking techniques for hiding data.

II. LITERARY ANALYSIS

With the recent advances in internet computing in our day to day life the need for communication has increased. Privacy in communication is desired when confidential information is shared between two parties. Without image security, we will end up giving our useful data to other people which may lead to some kind of loss. It is easy to transmit and duplicate, but unauthorized reproduction becomes a serious problem.
Over the years various researchers have proposed numerous methods for securing digital images for transmission. Naor et. al. [1] proposed a visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into n noise-like shares. The secret image can be decrypted by the human eye when any k or more shares are stacked together. The greatest advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is a simple and safe secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the share-images are larger than the original secret image. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry. Since the concept of visual cryptography was first proposed, there have been several studies making efforts to deal with the pixel expansion problem [2-11]. Most of these have fallen into the category of probability visual cryptography schemes.

Ito et al. [2] and Yang [5] used the concept of probability to interpret the meaning of the Boolean matrices proposed by the conventional VC and proposed a pixel non-expansion method suitable for binary images. However, the random nature of probability means that the shares have poor display quality. Tu and Hou [4] adopted Ito's method [2] but utilized multiple successive pixels in the secret image as the unit of encryption. They generated smooth-looking shares of invariant size for gray-level secret images.

In 1987, Kafri and Keren [6] proposed a random grid visual secret sharing (RGVSS) method, which has gained more attention over the years. In their method, each pixel of the image is treated as a grid, with a random variable used to encrypt the secret image. The biggest benefit of the RGVSS method for encryption is that it generates unexpanded share-images. In 2007 Shyu [7] extended Kafri and Keren's RGVSS model, proposing three different models utilizing a (2,2)-threshold scheme. Shyu [8] and Chen and Tsao [9] also presented (2, n)- and (n, n)-threshold RGVSS schemes, so this method is no longer limited to the (2, 2)-threshold scheme. Both traditional VC and RGVSS produced meaningless share-images, which can create some management problems for those participating in many secret sharing projects because they have to keep track of many different share-images.

Moreover, transmission of a meaningless image can arouse the suspicion of an outsider, who may realize that this image may carry some type of secret message. This attracts attention and could strengthen their desire to uncover the secret image, thus reducing the security of the share-image. Ateniese et al. [13] first applied the strategy of steganography to generate meaningful share-images in VC. Following Ateniese, Hou and Wu [14] proposed a method which uses the halftone and color composition/decomposition techniques to generate meaningful grey or color share-images. Zhou et al. [15] and Wang et al. [16] also improved upon Ateniese's method by developing VC algorithms for dealing with halftone images designed to make the recovered stack-

image less unclear. Chang et al. [17] found a way to hide a color secret image in two color cover images.
Nakajima and Yamaguchi [18] presented a scheme for encrypting a natural image. All of above methods used pixel expansion method to generate meaningful color share-images. For example, with the methods of Chang et al. [17] and Nakajima and Yamaguchi [18], pixel expansion made the share images nine times larger than the original image. Fang [19] proposed a progressive VC scheme which could also produce meaningful share-images, but pixel expansion meant that they were still four times larger than the original image. Thien and Lin [20] proposed a pixel non-expansion method that could produce a meaningful share-image but a computer was needed to decrypt the secret image, losing the advantage of visual cryptography which is decryption directly by the human eye.

Chen and Tsao [10] first proposed a user-friendly random grid visual secret sharing (Friendly RGVSS) method which achieved the goal of producing meaningful share-images and pixel non-expansion, but their method still had many restrictions. In that method, pixels are taken from the secret image and the cover image to generate the needed share-images. The result is that the contrast in the stack-image and share-images is not as good as that obtained with methods that use all the pixels to display the secret image or the cover image (e.g., Ateniese et al.'s EVCS). In extreme situations, when an insufficient number of black pixels are taken from the secret image, it may be impossible to display the content of the secret-image in the stack-image. In addition, with this method, only one picture can be used as the cover image, and the colors of the two share-images must be complementary to each other.

Lou et al. [11] proposed a visual secret sharing scheme capable of hiding a secret image and an extra confidential image within two meaningful cover images. The two share-images could be stacked to obtain the secret image without any complex computation. The shifting of one of the share-images by a certain unit could allow the receiver to obtain an extra confidential image with which to check the validity of the revealed secret image. However, with this system the visual quality is poor, because of the extra image hidden in the share-images, and the cover image cannot be concealed when the share-images are stacked. All these disadvantages reduce the visual quality of the share-images and the stack-image. Lee and Chiu [12] proposed an extended visual cryptography algorithm for general access structures to create unexpanded meaningful shares to hide a secret image. It operates in two phases. In the first phase, based on a given access structure and conventional VC schemes, meaningless shares are constructed by using an optimization strategy. In the second phase, cover images are directly added to each share by a stamping algorithm to generate meaningful shares. However, the ratio of incremental pixel density of the cover image to be stamped on the shares will heavily influence the contrast in the share-images and the stack-image. Increasing the contrast of the share-image will always decrease the contrast of the stack-image, and vice versa.

Apart from cryptographic encryption schemes as discussed above, watermarking is another method to secure image. Many researchers have used this technique for security purposes. Digital watermark is a kind of technology that embeds copyright information into multimedia data. According to watermark embedding position, digital watermark could be divided into two main kinds of spatial domain and frequency domain. Spatial domain digital watermark has more data quantity and more frangible than frequency domain digital watermark so that the research of digital watermark is centralized in frequency domain. Wavelet transform is a new time-frequency analyzing method to localize spatial and frequency domain. Many watermark algorithms are implemented in discrete wavelet transform (DWT) domain.

Peyman et. al. [21] proposed a technique to protect digital identity documents against a Print Scan attack for a secured ID card authentication system. The existing PS operation imposes several distortions, such as geometric rotation & histogram distortion on the watermark location which may cause the loss of information. The proposed system removes distortion of the PS operation: filtering, localization, binarizitation, rotation and cropping. The proposed authentication system extracts the watermarks inside the ID card's holder photo, place in the decoder and then checks it out with the ID card personal number. If the extracted watermark and the ID card personal number are the same, the identity of the user / customer will be verified otherwise identity will be denied.

Swathi etl al. [22] proposed a technique in which binary image was the watermark. In the frequency domain, the

embedding process on QR code image using watermark is performed. The QR code image is decomposed by one level using one dimensional wavelet transformation. Suhail et. al. [23] proposed a watermarking algorithm based on the discrete cosine transform (DCT) and image segmentation. The image was first segmented in different portions based on the Voronoi diagram and features extraction points. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment.

Tianming et. al. [24] presented a digital watermarking algorithm based on the DWT coefficients. This algorithm does not change any information of the original image, but combines the information of low frequency DWT coefficients and the watermark image. The combination is the key, which is used to extract the watermark. When we need to extract the watermark, we can obtain it by divide the key.

Yang et. al. [25] proposed a watermarking algorithm based on integer wavelet transform (IWT). Instead of hiding data bits directly to the blocks, authors employed adaptive bit-labeling scheme to a block so that it can be used to carry a data bit 0 or 1.

Wei et. al. [26] proposed a technique to embed digital watermark based on modifying frequency coefficients in discrete wavelet transform (DWT) domain. The authors discuss how to embed a 1-bit digital image as watermark in frequency domain. Also, a digital watermarking method is given in which 3-D DWT is used to transform a given digital image. Based on the experimental results, it is shown that the proposed methods are robust to a large extent.

Laskar et. al. [27] proposed a a robust digital image watermarking algorithm based on joint Discrete Wavelet Transform and Discrete Cosine Transform (DWT-DCT). The proposed system provides imperceptibility and higher robustness against common signal processing attacks. A binary watermarked image is embedded in certain subbands of a 3-level DWT transformed coefficients of a host image. Then, DCT coefficients of each selected DWT subband is computed. A randomly generated two-dimensional key is used to encrypt the watermark. This 2D key provides security to the image and ownership copyrights. The PN-sequences of the encrypted watermark bits are embedded in the coefficients of the corresponding DCT middle frequencies providing higher security. In extraction stage, the same approach as that of the embedding process is used to extract the DCT middle frequencies of each subband. Finally, correlation between mid-band coefficients and PN-sequences is calculated to determine watermark bit which is again post-processed by the two-dimensional key generated to derive the actual watermark.

Shi et. al. [28] adresses the problem that traditional digital watermarking algorithm based on DWT generally embedded in high frequency watermarks; these bands of wavelet coefficients are generally lower and they are vulnerable when attacked by different kinds of pictures so that they are difficult to deal with some strong attacks against algorithms such as damage to compression, filtering and so on. It results in that the robustness of algorithm always can't satisfy the requirements of practical application. The part of low-frequency after using Wavelet Transformation embeds in watermark information can improve the robustness of digital watermarking preferable by analysis. Under the condition that the amount of information in digital watermarking getting smaller, optimizing the image of Arnold scrambling algorithm, using it in to encrypts digital watermarking images, combining with the characteristics of singular value decomposition and processing the singular decomposition of wavelet transform image can enhance the digital watermark invisibility and robustness effectively.

Gonge et. al. [29] discussed a robust and secure DWT-SVD digital image watermarking using encrypted watermark for copyright protection of cheque image. First, the problem of security, ownership and copyright protection during digital data transmission is discussed. To overcome this problem, digital watermarking is used. During transmission of data, there are many attacks occurring either intentionally or non-intentionally on digital watermarked image. These results into degradation of image quality and watermark may get destroyed. To provide security to watermark private key encryption and decryption is used. This encrypted watermark is used further for digital watermarking process using combined DWT-SVD transform. In the paper, digital watermarking technique is used to provide ownership & copyright protection for cheque image and private key encryption & decryption technique used for security of bank watermark.

Rajeev et. al. [30] provided a compartive analysis of two techniques for watermarking. The watermarking was performed with gray image in transform domain to compare discrete wavelet transform (DWT) and discrete Mojette transform based on the quality measures like peak signal-to-noise ratio (PSNR) and mean square error (MSE). The proposed work also deals with a review of the various attacks on the watermarked image to alter the watermark, to remove, and to degrade the quality of the watermark in both cases.

Thind et. al. [31] proposed a hybrid video watermarking scheme which combines Discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) in which watermarking is done in the high frequency sub band and then various attacks have been applied.

Malonia et. al. [32] used DWT for watermarking. A cover image is decomposed into low and high frequency components by the application of 1-level Discrete Wavelet Transform. Average of each subband is calculated. The watermark is embedded into the 1-level high-high, high-low, low-high subband of cover image using Arithmetic Progression technique. The subband which has the smallest average is to be embedded first. After that, the watermarked image is projected to several attacks like median filtering, JPEG compression, Gaussian low-pass filtering, shearing, cropping, rotation etc. with different distortion strengths. The watermark which is embedded in the middle frequency subbands and high frequency subband is taken out by similar mechanism. The imperceptibility and robustness of the watermarked image is checked out by measuring the Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index values. From the implementation results, authors concluded that proposed watermarking algorithm can withstand many image manipulations compared to other existing DWT based methods.

III. TECHNIQUES

In this section, (2,2) Visual Cryptography scheme and watermarking using int-to-int DWT are discussed. Along with these, watermarking using DCT is also explained.

A. (2,2) Visual Cryptography Scheme

Visual Cryptography (VC) is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares.

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 or four sub-pixels as shown in Figure 2. 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 as shown in Figure 2.

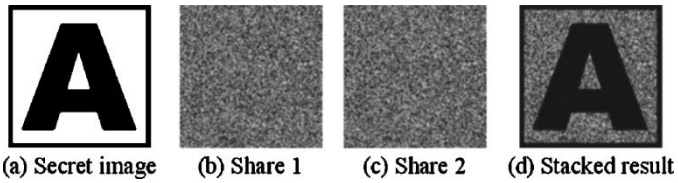


Figure 2: Working of visual cryptography scheme

1: (2, 2) – Threshold VCS: This takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.
2: (2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.
3: (n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.
4: (k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

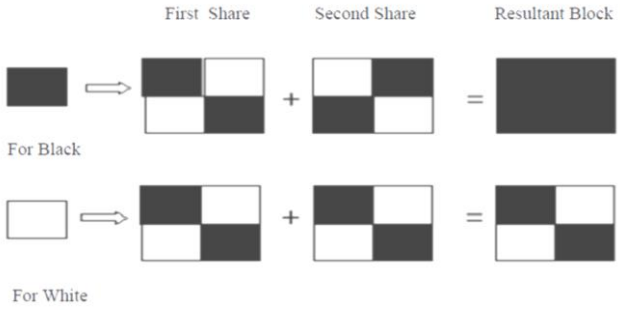


Figure 3: Encryption Rules Example

B. Digital Watermarking based on DCT

The discrete cosine transforms (DCT) are mathematical function that transforms digital image data from the spatial to the frequency domain. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is specified for lossy compression. DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. The expression for 2D DCT is given below where symbols have their usual meaning.

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j) \quad (1)$$

The DCT of the cover image is computed block by block where each block is of 8x8 pixels. The shares are embedded into the DCT transformed image at specific positions.

A. Digital Watermarking using IWT

Discrete wavelet transform performs multi-stage signal decomposition. Discrete wavelet transform using filter bank is shown in Figure 4.

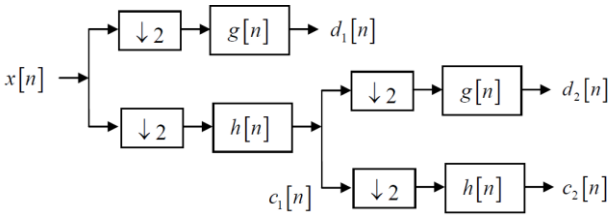
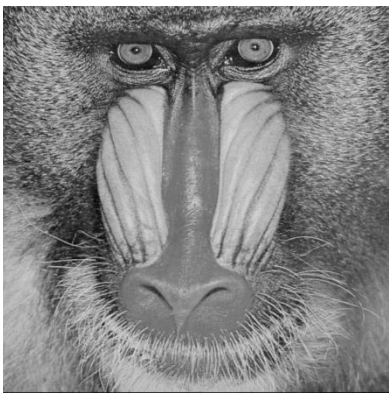


Figure 4: DWT Forward Transform Filter Bank

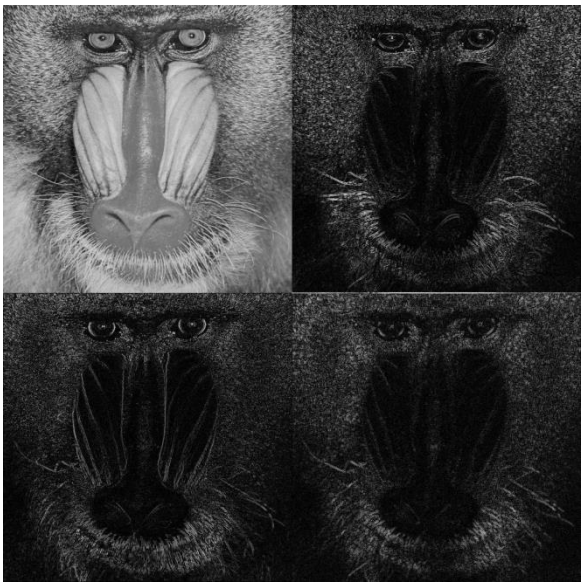
In this section, fast and efficient way of finding discrete wavelet transform using lifting scheme is discussed. It de-correlates the signal at different resolution level. Basic polynomial interpolation is used to find high frequency values. It is also used to construct scaling functions in order to find out low frequency values. Lifting scheme for Integer Wavelet Transform consist of three steps as shown in Figure 5.

- Split (Lazy wavelet transform)
- Predict (Dual lifting)
- Update (Primal lifting)

To obtain an efficient implementation of the discrete wavelet transform, it is of great practical importance that the wavelet transform is represented by a set of integers. Because if we store wavelet coefficients as a floating point values it requires 32 bits per coefficients. Hence, wavelet coefficients are rounded to convert it into integer number for efficient encoding and storage.



(a)



(b)

Figure 5: DWT decomposition (a) Original Image (b) First Level Decomposition Tree

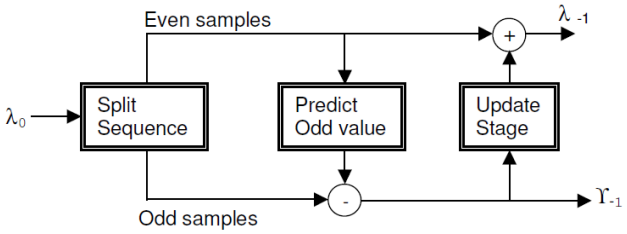


Figure 6: IWT Forward Transform

IV. ALGORITHMS

In this section, algorithms for (2,2) - Visual Cryptography Scheme and watermarking using Integer Wavelet Transform (Lifting Scheme) are discussed.

A. Steps for Visual Cryptography

1) Read the secret image (black & white).

2) Initialize two primary blocks which are complement to each other for creating shares. An example is

$$block\ 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (2)$$

$$block\ 2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

If these blocks are used, the shares will be twice the size of the secret image i.e., for each pixel in the secret image, there will be four pixels in each share.

3) Repeat the following for each pixel in the secret image,

a. If the pixel in secret image is 1, assign the corresponding four pixels in both the shares as block 1 or block 2 with equal probability.

b. If the pixel in secret image is 0, assign the corresponding four pixels
in share 1 as block 1 or block 2 with equal probability.
and in share 2 as block 2 or block 1 with equal probability.

4) Combine both the shares by concatenating the shares vertically.

B. Steps for Encryption using Integer to Integer DWT (Lifting Scheme)

1) Read the watermark image.

2) Compute the int-to-int DWT of the watermark image.
Parameters of Lifting Scheme:
Type : int2int
Wavelet : haar
Primal elementary lifting step: -0.125 , 0.125

3) Embed the combined share data in the Diagonal Detail component (HH component).

4) Now, reconstruct the image using the new Diagonal Detail component.

V. CONCLUSION

Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text.

Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Over the years various researchers have proposed numerous techniques for securing digital images for transmission. This paper discussed two classes of these algorithms, Cryptography and Watermarking. For

cryptography, VCS and its derived techniques were focussed. For watermarking, Integer wavelet transforms and discrete cosine transform based techniques were discussed. It may be observed that these techniques are popular among researchers for their many advantages. It may also be concluded that while a lot of work has been done in these areas, there is still a lot of scope for future work.

VI. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, pp. 1-12, 1995.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A, no. 10, pp. 2172-2177, 1999.

[3] T. L. Lin, S. J. Horng, K. H. Lee, P. L. Chiu, T. W. Kao, Y. H. Chen, R. S. Run, J. L. Lai, and R. J. Chen, "A novel visual secret sharing scheme for multiple secrets without pixel expansion," Expert Systems with Applications, vol. 37, no. 12, pp. 7858-7869, 2010.

[4] S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," Imaging Science Journal, vol. 55, no. 2, pp. 90–101, 2007.

[5] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, vol. 25, no. 4, pp. 481-494, 2004.

[6] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, vol. 12, no. 6, pp. 377-379, June 1987.

[7] S. J. Shyu, "Image encryption by random grids," Pattern Recognition, vol. 40, no. 3, pp. 1014-1031, 2007.

[8] S. J. Shyu, "Image encryption by multiple random grids," Pattern Recognition, vol. 42, no. 7, pp. 1582–1596, 2009.

[9] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," Pattern Recognition, vol. 42, no. 9, pp. 2203-2217, 2009.

[10] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 11, pp. 1693-1703, 2011.

[11] D. C. Lou, H. H. Chen, H. C. Wu, and C. S. Tsai, "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares," Displays, vol. 32, no. 3, pp. 118-134, 2011.

[12] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1 part 2, pp. 219-229, 2012.

[13] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," Theoretical Computer Science, vol. 250, pp. 143-161, 2001.

[14] Y. C. Hou and J. H. Wu, "An extended visual cryptography scheme for concealing color images," in Proceeding of The 5th Conference on Information Management and Police Administrative Practice, Taoyuan, Taiwan, pp. 62-69, (in Chinese) 2001.

[15] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2453, 2006.

[16] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 383–396, 2009.

[17] C. C. Chang, W. L. Tai, and C. C. Lin, "Hiding a secret color image in two color images," Imaging Science Journal, vol. 53, no. 4, pp. 229–240, 2005.

[18] M. Nakajima and Y. Yamaguchi, "Enhancing registration tolerance of extended visual cryptography for natural images," Journal of Electronic Imaging, vol. 13, no. 3, pp. 654–662, 2004.

[19] W. P. Fang, "Friendly progressive visual secret sharing," Pattern Recognition, vol. 41, pp. 1410-1414, 2008.

[20] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 12, pp. 1161–1169, 2003.

[21] Peyman Rahmati, and Andy Adler, and Thomas Tran. ―Watermarking in E-commerc, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013

[22] Swathi.K, Ramudu.K, Robust Invisible QR Code Image Watermarking Algorithm in SWT Domai,

International Journal of Innovative Research in Computer and Communication Engineering, Vol.2

[23] M. A. Suhail and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model," in IEEE Transactions on Instrumentation and Measurement, vol. 52, no. 5, pp. 1640-1647, Oct. 2003.

[24] Gu Tianming and Wang Yanjie, "DWT-based digital image watermarking algorithm," Electronic Measurement & Instruments (ICEMI), 2011 10th International Conference on, Chengdu, 2011, pp. 163-166.

[25] C. Y. Yang, W. Y. Hwang and Y. F. Cheng, "IWT-Based Watermarking By Adaptive Bit-Labeling Scheme," Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, Harbin, 2008, pp. 1165-1168.

[26] D. Wei, Y. Weiqi, Q. Dongxu," Digital image watermarking based on discrete wavelet transform", Journal of Computer Science and Technology, Vol. 17, No. 2, pp. 129–139, 2002

[27] S. S. Gonge, A. Ghatol,"A Robust and Secure DWT-SVD Digital Image Watermarking Using Encrypted Watermark for Copyright Protection of Cheque Image", International Symposium on Security in Computing and Communication, pp. 290-303, 2015

[28] C. Rajeev, K. P. Girish, "Comparative Analysis of Digital Watermarking in Discrete Wavelet Transform and Mojette Transform", Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Advances in Intelligent Systems and Computing, Vol. 324, pp 667-672

[29] D. K. Thind and S. Jindal," A Semi Blind DWT-SVD Video Watermarking", Procedia Computer Science, Vol. 46, 2015, pp. 1661-1667

[30] M. Malonia and S. K. Agarwal, "Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression technique," 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, 2016, pp. 1-6.

[31] R. H. Laskar, M. Choudhury, K. Chakraborty, S. Chakraborty,"A Joint DWT-DCT Based Robust Digital Watermarking Algorithm for Ownership Verification of Digital Images", Computer Networks and Intelligent Computing, Springer Berlin Heidelberg, 2011

[32] F. Shi, Y. Shi and L. Lai, "Optimization on digital watermarking algorithm based on SVD-DWT," 2011 IEEE International Conference on Granular Computing, Kaohsiung, 2011, pp. 582-585.