Survey of High Image Security and Compression Encryption through Discrete Shearlet Transform and Block Truncation Code

Shrinidhi Tiwari[1], Prof. Ritu Ranjani Singh[2]

[1]M. Tech. Scholar, [2]Assistant Professor

Dept. of Computer Science & Engineering, Bansal Institute Science and Technology, Bhopal

Abstract*—"Watermarking" is a technique that thwarts unauthorized users to have access to the crucial data, to invisibility and payload capacity using the different technique like discrete cosine transform (DCT) and discrete shearlet transform (DST).The available methods till date result in good robustness but they are not independent of file format. The aim of this research work is to develop independent of file format and secure hiding data scheme. The independent of file format and secure hiding data scheme will increase by combining DST and least significant bits (LSB) technique. Accordingly an efficient scheme is developed and compressed the image with the help of golomb code vector quantization technique.

*Keywords— **Discrete Shearlet Transform, Golomb Code Vector Quantization***

I. INTRODUCTION

Recent growth of digital image content over internet has increased the need for the protection of digital media. The image transmitted through internet and wireless communication channels can suffer various threats. One of the major threats is the threat of confidentiality. This threat represents the possibilities of accessing the audio data via unauthorized channels. Another issue is the threat of integrity, where the resource can be altered, by unauthorized entities, without any detection. Threat of availability is possession of a confidential audio content through some illicit channels. Various other threats include replication of digital data without any information loss and manipulations of the same without any detection. A feasible solution is required, for telecommunication, consumer electronics and information technology industries, to provide secure transmission of content without sacrificing their security rights [1]. Emerging technologies for audio security has three main objectives: secure content transmission, authentication of audio information and copy control to protect audio data from illegal distribution and theft [2]. Cryptography has been established as a technology of fundamental importance for securing digital transfers of data over unsecured channels. By providing encryption of digital data, cryptography enables trustworthy point-to-point information exchange and transactions. Once the recipient validates and decrypts the data, the product can be subsequently stripped from any content identification, proof-of-ownership or other descriptive information. This might lead to further duplication and re-distribution leaving the rights holders powerless and royalty-less [3]. To enhance the security of audio data, digital watermarking and steganography techniques complement cryptography for protecting content even after it is deciphered [4].

The study of multimedia security [5] therefore includes not just encryption but also watermarking and steganography. Steganography and Watermarking almost interchangeably, refers to hiding secondary information into the primary multimedia source. The primary multimedia sources can be audio, image, and video. There are unique techniques associated with each type of primary perceptual sources depending on their inherent redundancy and perceptual properties. These techniques have been proposed as alternative methods to enforce the intellectual property rights and protect digital media from tampering [6]. In this thesis work the primary multimedia source is image.

The word steganography was originated from Greek which means covered writing. Steganography is the oldest form of covert channel. A famous illustration of steganography is Simmons' Prisoners' Problem [7]. Audio Steganography is the act of embedding a secret message within a larger message so that others cannot discern the presence of the secret message [8]. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. Audio watermarking involves a process of embedding into host audio signal a perceptually transparent digital signature, carrying a message about the host data in order to mark its ownership. The aim in watermarking systems is to ensure the robustness of the hidden message; the presence of the embedded message itself does not have to be secret [9].

The watermark is always present in the signal, even in illegal copies of it and the protection that is offered by the watermarking system is therefore of a permanent kind. Although the process of watermark embedding and steganography are similar, there are some basic differences between the two techniques. Steganography methods

assume that the existence of the covert communication is unknown to third parties and are mainly used in secret one-to-one communication between authorized users. On the other hand, watermarking is to hide message in one-to-many communications. Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Whereas, watermarking methods need to be very robust to attempts to remove or modify a hidden message.

II. LITERATURE REVIEW

Awdhesh K. Shukla et al. [1], a high limit information concealing technique utilizing lossless pressure, propelled encryption standard (AES), modified pixel esteem differencing (MPVD), and least significant bit (LSB) substitution is exhibited. Number juggling coding was connected on a mystery message for the lossless pressure, which gave 22% higher implanting limit. After pressure and encryption, the LSB substitution and MPVD are connected. It is tentatively settled that with the proposed strategy, significant upgrade in installing limit was accomplished and additional bits than existing strategies could be implanted because of the utilization of number juggling pressure and MPVD. The MPVD and number juggling coding together came about into 25% upgraded implanting limit than the prior strategies. The proposed technique likewise furnishes elevated amounts of visual quality with a normal of 36.38 dB at 4.00 bpp.

S. Thakur et al. [2], in this paper, we present a powerful and secure watermarking approach utilizing change space method for tele-wellbeing applications. The patient report/personality is inserting into the host medicinal picture with the end goal of verification, explanation and recognizable proof. For better secrecy, we apply the disorder put together encryption calculation with respect to watermarked picture in a less unpredictable way. Exploratory outcomes obviously shown that the proposed strategy is exceedingly hearty and adequate secure for different types of assaults with no huge contortions among watermarked and spread picture. Further, the execution assessment of our strategy is discovered better to existing cutting edge watermarking strategies under thought. Besides, quality investigation of the watermarked picture is assessed by abstract measure which is valuable in quality driven social insurance industry.

R. Srivastava et al. [3], this paper introduce a computationally productive joint intangible picture watermarking and joint photographic specialists gathering (JPEG) pressure conspire. As of late, the transmission and capacity of computerized archives/data over the unbound channel are gigantic concerns and almost the majority of the advanced reports are compacted before they are put away or transmitted to spare the transfer speed prerequisites. There are numerous comparable computational activities performed amid watermarking and pressure which lead to computational excess and time delay. This requests advancement of joint watermarking and pressure conspire for different interactive media substance. In this paper, we propose a strategy for picture watermarking amid JPEG pressure to address the ideal exchange off between significant execution parameters including implanting and pressure rates, strength and installing changes against various realized flag handling assaults.

D. S. Chauhan et al. [4], this paper present a protected restorative picture watermarking system applying spread-range idea in wavelet change space is proposed. In the initial step, discrete wavelet transform(DWT) deteriorates the spread restorative picture into four recurrence sub-groups utilizing Mexican cap as mother wavelet and after that comparing to every pixel of the parallel watermark a couple of Pseudo-Noise (PN) is installed into a level (HL) and a vertical (LH) sub-band. So as to keep up the indistinctness of the watermarked picture, quality of the produced PN arrangement pair is balanced by indicated report to watermark proportion (DWR). For the extraction the watermark, measurable profile of DWT coefficients of watermarked picture is resolved and the got likelihood dispersion work (pdf) is used for planning the watermark location system.

Table 1: Summary of Literature Review

Title	Author/ Publication	Methodology	Parameters
A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing	Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh, And Amod Kumar, IEEE 2018	Data hiding using encryption and optimized pixel difference method	PSNR = 37.32 dB, SSIM = 0.9403, Standard Deviation = 0.1465
Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications	S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, IEEE 2018	Security for medical image using chaotic encryption	PSNR = 34.72 dB, SSIM = 0.8403,
Computationally efficient joint imperceptible image watermarking and JPEG compression: A green computing approach	R. Srivastava, B. Kumar, A. K. Singh, and A. Mohan, IEEE 2017	JPEG compression using joint imperceptible method	PSNR = 33.88 dB, SSIM = 0.8803, Standard Deviation = 0.1665
Combining Mexican hat wavelet and spread spectrum for adaptive water-marking and its statistical detection using medical images	D. S. Chauhan, A. K. Singh, A. Adarsh, B. Kumar, and J. P. Saini, IEEE 2017	Security using wavelet and spread spectrum technique	PSNR = 31.32 dB, SSIM = 0.7803, Standard Deviation = 0.1365

III. DIGITAL WATERMARKING

Watermarking basically refers to information hiding. Information or digital signal in the form of images, audio, video or text is hidden or inserted. This information to be hidden is termed as Watermark. The watermark can be hidden in cover/host/carrier signal. The host popularly can be text file, image, audio file or video file. Depending on the type of host, watermarking can be categorized as:

- Text watermarking
- Digital image watermarking,
- Digital audio watermarking and
- Digital video watermarking

To have efficient copyright protection, watermarking algorithms must possess certain characteristics. Depending on the application requirement different characteristics can be primary objectives. The most desirable characteristics [2] are listed below:

Robustness- Robustness refers to difficulty in removing or destroying watermark from host image when watermarked image is subjected to image processing attacks.

Imperceptibility- Imperceptibility dictates the inability to notice the existence of watermark in host image and retained visual quality of host image after embedding watermark into it.

Capacity- Capacity refers to amount of information that can be embedded in host image. Capacity depends on the application and the image.

Security- Watermarking algorithm is secure if knowing the algorithm to embed and extract the watermark does not help an unauthorised party to detect the presence of watermark.

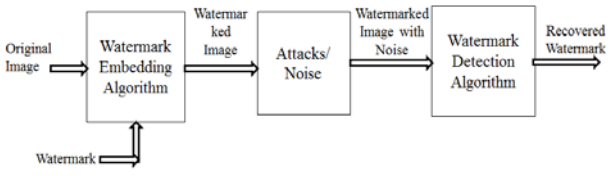

Figure 1: General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

All these characteristics cannot be achieved simultaneously as there is always a trade-off between them. For example, robustness and imperceptibility are contradictory to each other. Watermarking algorithm having high robustness usually sacrifices imperceptibility and vice versa. For higher robustness increased capacity is desired. But increased capacity leads to compromising imperceptibility. Watermarking methods introduced in proposed work aim to provide higher robustness as well as imperceptibility.

IV. DISCRETE SHEARLET TRANSFORM

Shearlet transform is an affine function containing a single mother Shearlet function that is parameterized by scaling, shear and translation parameters with the shear parameter capturing the direction of the singularities [8]. An important advantage of this transform over other transforms is due to the fact that there are no restrictions on the number of directions for the shearing. There are also no constraints on the size of the supports for the shearing, unlike, for instance, directional filter banks [9] where using a small window size would result in a performance loss. Therefore, the Shearlet transform is designed to deal with directional and anisotropic features, typically present in images, and has the ability to effectively capture the geometric information of edges.

In relation to its application for image watermarking, the DST ability to better represent directional features as claimed in [10], may allow watermark embedding to adapt to the diagonal features in the host image more efficiently. In this section, a new DST-based watermarking framework for blind watermarking is developed in order to explore the possible improvements on DST performance against signal processing, geometric and compression based attacks. In addition, this proposed new blind watermark detection scheme for DST coefficients is optimal for non-additive schemes relying on the statistical decision theory.

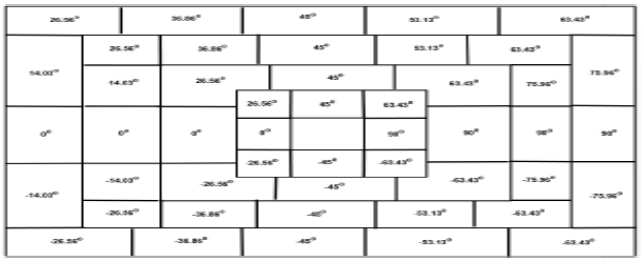

FIGURE 2: 2- LEVELS FOR DST.

The DST of the first flag is then gotten by connecting all coefficients beginning from the last level of decay (staying two examples, for this situation). The DST will then have an indistinguishable number of coefficients from the first flag.

V. PROPOSED METHODOLOGY

DST involves decomposition of image into frequency channel of constant bandwidth. This causes the similarity of available decomposition at every level. DST is implemented as multistage transformation. Level wise decomposition is done in multistage transformation.

S is a diagonal matrix of singular values in decreasing order. The fundamental thought behind SVD strategy of watermarking is to discover SVD of picture and the

modifying the particular incentive to insert the watermark. In Digital watermarking plans, SVD is used due to its basic properties:

A s mall aggravation incorporated the photo, does not cause tremendous assortment in its singular characteristics. The particular esteem speaks to inborn logarithmic picture properties [3].

LSB Technique:-

This technique works best when the file is longer than the message file and if image is grayscale.

When applying LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

$$S(i, j) = C(i, j)-1, \text{ if LSB } (C(i, j)) = 1 \text{ and } SM = 0$$

$$S(i, j) = C(i, j)+1, \text{ if LSB } (C(i, j)) = 0 \text{ and } SM = 1$$

$$S(i, j) = C(i, j), \text{ if LSB } (C(i, j)) = SM$$

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and "SM" id the next message bit to be embedded. S(i, j) is the Stego image.

The proposed method follows a directional embedding technique for achieving maximum image quality in the stego image. The proposed method performs a selection of suitable direction for secret byte embedding so as to minimize the bit changes in the cover image when a secret data is embedded.

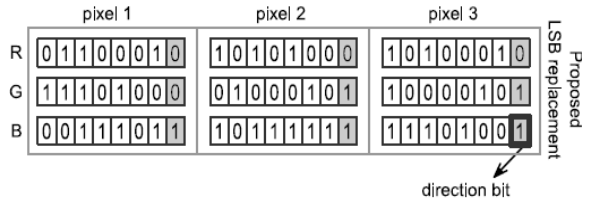

Figure 3: LSB embedding of the byte 11110000 in the cover image using the proposed method.

As you can see in Fig. 4, the byte 11110000 is embedded in a reverse order (00001111) in the original cover image for minimizing the number of alterations. Here also, we take three consecutive pixels (say *p*1, *p*2 and *p*3) for embedding a byte of information. Firstly, the red channels of *p*1, *p*2 and *p*3 are replaced with secret bits, followed by their green and blue channels. A direction bit is added at the 9-th bit which indicates that the preceding data is in stored in a reverse order. A value for the direction bit indicates a normal forward direction of storing data while a value 1 for the direction bit indicates that the data is stored in reverse direction.

Golomb Code Vector Quantization

An efficient representation of integers is essential in many applications such as text compression, image compression, fast query evaluation, fast searching, and fast file access, In all these applications, one of the simple algorithms such as Golomb coding, Elias coding, Fibonacci coding etc, is used to represent an arbitrary integer compactly. The selection of the algorithm depends on the type of application and the probability distribution of the integers in that application. We can also construct variable length codes using the above mentioned simple algorithms without knowing the probability of the integers in advance. While many different representations have been developed, it is not always obvious in which circumstances a particular code is to be preferred.

The proposed new variable length code, called Extended Golomb Code (EGC), is presented to code the given non-negative integer N. In EGC, a divisor (d) is selected and the integer N to be coded is divided successively M times by d until the quotient q becomes zero. In each division, the remainders r_i (i = 1 to M) are retained. The integer N is then coded by coding M and the M remainders as

$$\text{Code (M)} = \text{Code } (r_M, r_{M-1} \ldots r1)$$

M is coded in unary and the remainders (r_M, r_{M-1} …r1) are coding using a unique coding scheme. The bit length bl of EGC follows the inequality:

$$bl \leq (\left|\frac{\log_{10} N}{\log_{10} d}\right| + 1) * (1 + Log_2 d)$$

In general, when an integer N is divided by a divisor d, there are d possible remainders when the quotient (q) is greater than 0, and d-1 possible remainders when q is equal to 0.

Algorithm for Encoding

The integers in file to be compressed are encoded using following steps:

1. Select an optimized divisor (d) for the probability distribution of the integers in that file.
2. Divide each integer N successively by d, until the quotient (q) becomes zero. Count the number of divisions made as M. Retain the remainders in each division as r_1, r_2, r_3… r_M. Code r_1, r_2, r_3… r_{M-1} in $\log_2 d$ bits, and r_M in $\log_2 (d-1)$ bits.

Algorithm for Decoding

The following steps are used to decode the data in the compressed file.

1. Read the next bit 0 until bit 1 is encountered and count the no. of reads made so far including the bit 1 as M.
2. Read the bits further and decode M remainders as per the code given for the given divisor d and reconstruct r_i.
3. Then obtain the integer N using the following procedure

```
If      d > 2
{
        Set N = 0
        For i = M to 1
            N = N*d + ri
}
Else
{
         Set N=1
For          i = M-1 to 1
              N = N*d + ri
}
```

Repeat the steps 1 and 2 to obtain all Ns in the compressed file.

VI. CONCLUSION

It has been proved that the use of DST-SVD with image compression technique method has improved the security of the watermarking scheme. Particular attention is given to the proposed scheme to from the above descriptions, it have been shown that using Watermarking can ensure a secure message.

REFRENCES

[1] Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh, And Amod Kumar, “A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing”, Received July 5, 2018, accepted August 25, 2018, date of publication September 3, 2018, date of current version October 8, 2018.

[2] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, ``Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," in *Multimedia Tools and Applications*. New York, NY, USA: Springer, 2018, pp. 1_14.

[3] R. Srivastava, B. Kumar, A. K. Singh, and A. Mohan, “Computationally efficient joint imperceptible image watermarking and JPEG compression: A green computing approach," *Multimedia Tools Appl.*, vol. 77, no. 13, pp. 16447_16459, 2017.

[4] D. S. Chauhan, A. K. Singh, A. Adarsh, B. Kumar, and J. P. Saini, “Combining Mexican hat wavelet and spread spectrum for adaptive water-marking and its statistical detection using medical images," in *MultimediaTools and Applications*. New York, NY, USA: Springer, 2017, pp. 1_15.

[5] N. Senthil Kumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique”, International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[6] Aase, S.O., Husoy, J.H. and Waldemar, P. (2014) A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[7] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[8] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[9] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.

[10] Al-Otum, H.M. and Samara, N.A. (2009) A robust blind color image watermarking based on wavelet-tree bit host difference selection, Signal Processing, Vol. 90, Issue 8, Pp. 2498-2512.

[11] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. (1996) Visual cryptography for general access structures, Information Computation, Vol. 129, Pp. 86-106.

[12] Baaziz, N., Zheng, D. and Wang, D. (2011) Image quality assessment based on multiple watermarking approach, IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5.

[13] Bao, F., Deng, R., Deing, X. and Yang, Y. (2008) Private Query on Encrypted Data in Multi-User Settings, Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC 2008), Pp. 71-85, 2008.

[14] Barni, M. and Bartolini, F. (2004) Watermarking systems engineering: Enabling digital assets security and other application, Signal processing and communications series, Marcel Dekker Inc., New York.

[15] Barni, M., Bartolini, F. and Piva, A. (2001) Improved Wavelet based Watermarking Through Pixel-Wise Masking, IEEE Transactions on Image Processing, Vol. 10, Pp. 783-791.