Simulation of High Security Text with Digital Image Watermarking with Image Segmentation

Bhagyashree Patil[1], Dr. L. K. Vishwamitra[2]

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

OCT, Bhopal

Abstract - Watermark is the technique to secure the image and Steganography is the science where the secret data in multimedia payload, such as text, image, audio and video that conceal the existence of communication. The aim of this work is to explore the enhancement of watermark and steganography by combining text and image formation to achieve, imperceptible, encryption, security and robustness in the area of digital images. Our proposed work investigates that digital watermarking and steganography enhancement by combining text and image through Discrete Shearlet Transform (DST). The existing metrics in data hiding like PSNR, NAE and MSE are having primary objectives such as the embedded data must be imperceptible to the observer, where a high PSNR and low MSE and NAE indicates that the stego image is closer to the original different types of file format image. Results demonstrate that our system successfully hides and recovers a significant amount of secret message within digital images with Gaussian and Salt and Pepper noise attack. For many experimental on combining text and image, the performance of this system falls between other researchers where, the proposed system gives higher PSNR value.

I. INTRODUCTION

The term water marks got its name toward the finish of the eighteenth century as it takes after the impacts of water on paper. Emil Hembrooke documented a patent in 1954 which was for recognizing music works was the main case of innovation like computerized water checking, Komatsu and Tominaga utilized the expression "advanced watermarking" in 1988 first. The term water marks got its name toward the finish of the eighteenth century as it takes after the impacts of water on paper. Emil Hembrooke recorded a patent in 1954 which was for recognizing music works was the primary case of innovation like advanced water checking, Komatsu utilized the term [6].

The idea of communicating secretly is as old as communication itself; the old examples of secret writing are allusion by Homer‟s Iliad, Arthasastra by Kautilya, writing by sympathetic inks such as milk, lemon and others. The origin of steganography is biological and physiological. Linguistic steganography consists of linguistic or language forms of hidden writing, it is also called as semagrams. It recognizes two methods, a secret message is either made to appear innocent in an open code or it is expressed in the form of visible graphical details in a script or drawing in a semagram. Watermarking techniques has evolved from steganography[7].

Figure 1.1: Watermark in Mark and Dollar Bank Notes

II. LITERATURE REVIEW

Devices such as I-pod, Mobile phone, Web Camera, Personal Digital Assistant, Digital camcorder and others allow the users in an interactive way to create, modify, delete and view digital data. A new invention provides more features in a single device and provides very high portability. These inventions and developments create an electronic environment where the user can share and deliver the multimedia content, but it also decreases the authenticity of the content. Also with the rapid growth of Internet technologies and wide availability of multimedia computing facilities, the enforcement of multimedia copyright protection becomes an important issue. Digital information can be perfectly copied and is easily stored which makes it onerous to enforce the negotiated rights and conditions for use of the data. In this situation, protection of digital.

Bidyut JyotiSaha et al. [7],they have proposed secure algorithm to protect the watermark image over a public network in digital watermarking and is embedded in Discrete Wavelet Transformation (DWT). Unlimited growth in internet and multimedia leads to large usage of images resulting in huge storage and distribution of multimedia contents. With increasing use of digital transmission techniques the potential risks for multimedia content is high which lead to necessity of protection for authenticity and confidentiality.

M. Kim et al. [8],they have proposed new blind watermarking scheme by quantizing the singular values of wavelet component. in recent years, singular value

decomposition has become a popular tool for image watermarking. To optimize the system performance, treat the image watermarking as a multi-objective optimization problem based on non-dominated sorting genetic algorithm II. Based on this new perspective, the inherent conflict existing in image fidelity and watermark robustness for image watermarking can be objectively handled. The experimental study shows that our methods indeed provide superior performance.

Jiann Shu et al. [9],they have proposed new non-blind digital image watermarking method for embedding a binary logo in an image, based on the dual-tree complex discrete wavelet transform (DT-CDWT) and interval arithmetic (IA). As our experimental results demonstrated, since the high-frequency components obtained by using DT-CDWT and IA contained a low-frequency component, we may expect that the image quality and robustness is maintained even if we embed the watermark into the high-frequency components.

BaloshiMathews et al. [10],they have proposed novel DCT-based watermarking, in which binary visually meaningful information is embedded into the cover image to detect temperament. Initially, researchers worked with watermark encryption using a single chaotic map. This technique is used to embed each byte information of watermark image in each DCT block by shifting any random coefficient to have a mapped value in a binary mapping coefficient function which is same as watermark bit.

Wang Santosh et al. [11], they have proposed a non-blind watermarking scheme by taking 1D logistic chaos equation in DWT domain. Here, they have focussed on the low frequency part to embed information. 1D Logistic map is used to encrypt the original watermark image. The encrypted watermark image is embedded into lower frequencies of DWT coefficients. For watermark detection, correlation between the watermark to be tested for presence, and the marked coefficients is computed. The same watermark information is embedded into different sub bands and in different levels to make it resilient against various attacks. **Lee et al. [12]**, they have proposed an efficient and secure data hiding technique. The paper proposed a technique to compress and hide the secret message using Huffman coding. Each symbol in the cover medium can carry one secret bit. The secret message is also encrypted using logistic map with a secret key before embedding. First, singular values in a digital image have very good stability, that is, when a small perturbation is added to image, its singular values do not change significantly. Second, singular values contain intrinsic algebraic image properties. Each singular value specifies the luminance of image while the corresponding pair of left and right singular vectors specifies the geometry of the image layer.

III PROBLEM FORMULATION

Watermark is embedded into a host image, if we crop or damage the watermarked image, the recipient would not be able to extract the complete watermark. The extracted watermark will be distorted and some important information may be lost. To overcome the loss of information, we can rearrange the pixel sequence of a watermark via a random sequence generator [1]. Although the random sequence generation can rearrange the pixel permutation of a watermark, it does not spread the neighbouring pixels into dispersed locations sufficiently. As a result, the relocated pixels are still close to one another. In order to spread the neighbouring pixels into largely dispersed locations, we often use the chaotic map. In mathematics and physics, chaos theory deals with the behaviour of certain nonlinear dynamic systems that exhibit a phenomenon under certain conditions known as chaos [2,3], which adopts the Shannon requirement on diffusion and confusion [4]. Chaotic maps take the parameters either in discrete-time or continuous-time domain. Iterated functions are used to form discrete maps. Characteristics of chaotic maps are well taken in robust digital watermarking to enhance the security. The most critical aspects of chaotic functions are its utmost sensitivity to initial conditions and its outspreading behaviour over the entire space. Therefore, chaotic maps are very useful in watermarking and encryption [5]. Though the values generated from the chaotic functions are limited within a range, they are totally random in nature and never converge.

3.1 Types of Digital Watermarking :- Based on the domain of usage, the watermarking techniques are grouped as spatial and frequency domain watermarking. Based on the content type of digital documents, the watermarking techniques are classified as text, image, audio and video watermarking. Also based on Human Perception the watermarking techniques are further classified as visible and invisible watermarking, the invisible watermarking is further classified as robust and fragile watermarking. Robust watermarking is further

3.1 CLASSIFICATION OF WATERMARKING ATTACKS :- A wide variety of attacks both incidental and malicious should be survived by a robust watermark. Some of the best known attacks are introduced as under [19].

3.1.1 Simple Attacks P:- Attacks like waveform or noise are aiming at damaging the fixed watermarks by manipulating the data as of whole watermark (watermark with host data) without any effort to identify & isolate the watermark. For instance addition of an offset, compression

(MPEG, JPEG), with addition of noise, filtering is cropping and same to the data conversion and Digital to analog[20].

3.4.2 Attacks of Detection-disabling :- The attacks of synchronization are used to break the correlation. A watermark detector finds it impossible or infeasible to recover the watermark. It is done by the synchronization attacks mostly by geometric distortion like, rotation, pixel permutations, shift in direction (for video), cropping, subsampling, insert of pixel clusters or pixels, removal of pixels or pixel clusters or gathering some geometric data[21].

3.4.3 Ambiguity Attack :- Fake watermark data occur on attack, inserting fake watermark, these fake watermarked data create some confusions. An inversion attack which tries to discredit the authority of the watermark by fixing one or several extra watermarks from which one cannot know the first authoritative watermark.

3.4.4 Removal Attacks :- To discard only the watermark, to separate the watermark data into host data and watermark to estimate the watermark or the host data and to analyze the watermark data, the removable attacks are attempted for the above fulfilment. Examples are collusion attacks, de-noising, certain filter operations, or compression attacks using synthetic modelling of the image.

3.5 WATERMARKING SYSTEMS OF ROBUST

Against wide range of unintentional and intentional image processing operations such as image filtering, enhancement, JPEG compression, noise addition, collusion, geometrical transformations, and forgery attacks [23], a robust watermarking system is resilient.

3.5.1 Attacks on Robust Watermarks :- To perform attacks on the toughness of the watermarking systems can be made possible by the availability of wide range of unique processing software.

3.5.2 Degradation of Image :- The robust watermarks are damaged by these types of attacks by removing parts of the image. The watermark information may be carried by the parts that are replaced.

3.5.3 Enhancement of Image :- The watermark information in an image is desynchronized by these attacks that are convolution operations. These attacks include sharpening, histogram, smoothing, equalization, contrast enhancement and median filtering.

3.5.4 Compression of Image :- Images are generally zipped with JPEG2000 and JPEG compression techniques in order to minimize to storage space and cut the cost of bandwidth required for transmitting images. These lossy compression methods are more damageable as compared to lossless compression methods.

VII CONCLUSION FUTURE SCOPE OF WORK

The emerging techniques in the field of transform domain such as DST and adaptive Steganography are not an easy target for attaches, especially when the concealed messages are small. We have proposed a new framework for enhancing security system by combining text and image, in which a new digital watermark and steganography method based on DST, shows the effectiveness and robustness of the proposed system. As future work more focus can be on improvement of compression ratio by using new techniques. The proposed technique can be experimented on various kinds of datasets like audio, video, text as till now it is only restricted to images. New methods can be combined and proposed to decreases the time complexity incurred in creating dictionary in LZW Algorithm. The experimental dataset in this research is limited; so applying the developed method on a larger dataset could be a subject for future research which may lead to new observations and conclusions.

IV PROPOSED METHODOLOGY

A digital image consists of a set of pixels, which can be conveniently captured using any electronic device, such as a camera, scanner or camcorder. With the increased use of the Internet and proliferation of image capturing devices, the access and distribution of images has become convenient and tremendously attainable.

4.1 Watermarking Embedding Procedure :- The procedure for embedding the watermark that following in this work is given as follows:

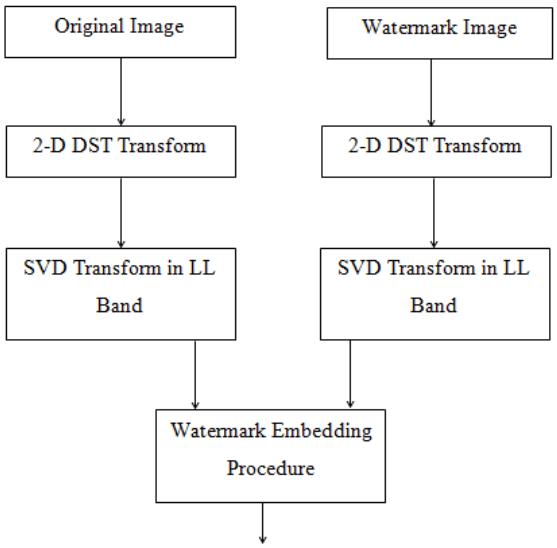

Figure 4.1 The Watermarking Embedding Procedure

- Select the host and the watermark image.

- Apply DST transform on both original and the watermark image.
- Apply SVD on the LL sub band of both original and the watermark image.
- Embedding process

4.2 PROPOSED ALGORITHM :-

Step 1: Take host image as input and convert it into Resize image original (RIO).

Step 2: Apply 2-D DST on resize image original (RIO) to decompose it into seven sub-bands.

Step 3: Select sub-band LL_2 of RI.

Step 4: Then apply SVD to sub-bands LL_2 to get UR, ΣR and V^TR.

Where U is real unitary matrix, Σ is rectangular diagonal matrix, V is complex unitary matrix, $V^T$is the conjugate transpose of **V** and R is Resize Image

Step 5: Take watermark image as input and convert it into Resize image watermark (RIW). Apply 2-D DST on resize image watermark (RIO) to decompose into seven sub-bands.

Step 6: Select sub-bands LL_2 of Wi.

Step 7: Then apply SVD to sub-bands LL_2 to get UW, ΣW and V^TW.

Step 8: Modify UR, ΣR and V^TR by using equation

UR* = UR + (0.10*UW);

ΣR* = ΣR + (0.10* ΣW);

$V^TR^* = V^TR + (0.10* V^TW)$;

Step 9: Construct modified SVD matrix UR*, ΣR* and V^TR^*.

Step 10: Apply inverse SVD.

Step 11: Apply inverse DST and finally get output image and secret message.

4.3 Noise Attack :-

Gaussian Noise: - Gaussian noising is a procedure that adds a commotion flag to a picture keeping in mind the end goal to intentionally degenerate the picture, thus diminishing its visual quality.

Salt and Pepper Noise: - Salt and Pepper noise represents itself as randomly occurring white and black pixels in an image.

Localvar Noise Attack: - Gaussian localvar shares many common properties with other smoothing processes.

Poisson Noise Attack: - Shot noise and poison noise attack is associated with the particle nature of light. Shot clamor in electronic gadgets comes about because of unavoidable irregular factual variances of the electric current when the charge transporters, (for example, electrons) navigate a hole.

V RESULTS AND DISCUSSION

MATLAB is a high level technical computing language and algorithm development tool that can be used in several applications such as data visualization/analysis, numerical analysis, signal processing, control design, etc.

5.1 SIMULATION PARAMETERS :- The mean square error (MSE) and the peak signal to noise ratio (PSNR) are used to measure the resulting error of watermarking image.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[y(i,j) - x(i,j)]^2$$

5.2 PSNR :- Peak signal to noise ratio, frequently truncated PSNR, is a designing term for the proportion between the greatest conceivable energy of a flag and the energy of adulterating clamor that influences the loyalty of its portrayal.

$$PSNR = 10\log_{10}\frac{M \times N}{MSE}$$

VI SIMULATION RESULTS

6.1 Salt and Pepper Noise Attack :- Figure 5.3; show the original Pepperimage of 512×512 pixel value. The random image of the original image is resized 512×512image, resize image is shown in figure 5.3 (a).

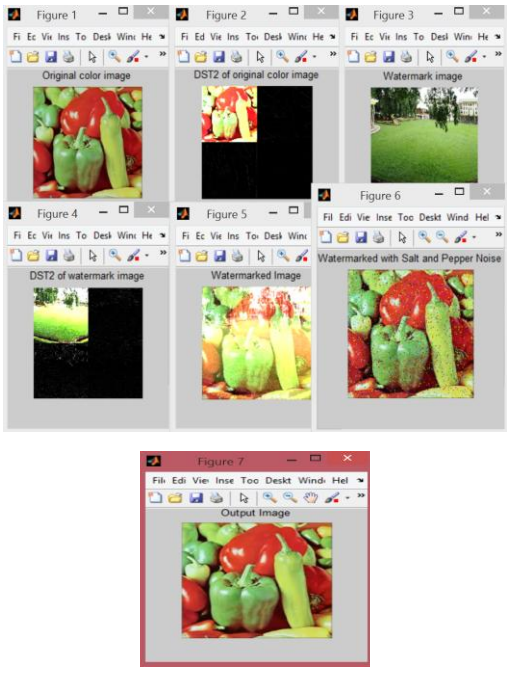

Figure 5.3: Experiment Flower Image with Salt and Pepper Noise

6.2 Result for Different Images without Noise Attack

Image	PSNR (dB)	MSE	NAE	Computation Time (ns)
College Image	35.289	77.561	18.652	4.674
Baboon Image	44.206	12.334	2.376	4.682
Pepper Image	34.069	28.519	10.005	4.093

The proposed DST-SVD technique gives a highest PSNR 44.206 dB for Baboon image and lower PSNR 34.069 dB for Pepper image.

6.3 COMPARISON RESULT

The peak signal to noise ratio (PSNR) result is obtained for the proposed DST-SVD technique and previous technique is shown in table 5.4. The proposed algorithm is gives 42.65 dB PSNR compared to previous algorithm 61.959 dB PSNR for Lena image. It is clear that the proposed algorithm 11.33% improvement of PSNR for previous algorithm.

	Previous Algorithm		Proposed Algorithm
Image	Scheme-I [1]	Scheme-II [1]	PSNR (dB)
College Image	42.65	41.24	55.743
Baboon Image	41.37	38.89	55.032
Pepper Image	42.65	41.38	54.943

6.4 CONCLUSION :- Steganography image bit is introduced in our proposed method. Images after extracting the embedding secrete message is nearly the same with the original image before embedding in aspect of recognition result. This thesis also provides a new approach to inverse key-based steganography techniques, which are grouped based on the usage of secret keys.

6.5 FUTURE SCOPE OF WORK :- As future work more focus can be on improvement of compression ratio by using new techniques. The proposed technique can be experimented on various kinds of datasets like audio, video, text as till now it is only restricted to images. New methods can be combined and proposed to decreases the time complexity incurred in creating dictionary in LZW Algorithm.

VII REFERENCES

[1] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption”, Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[2] BaharakAhmaderaghi ; FatihKurugollu ; Jesus Martinez Del Rincon ; Ahmed Bouridane, “Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory”, IEEE Transactions on Computational Imaging, Volume: 4 , Issue: 1, Page s: 46 – 59, IEEE 2018.

[3] AlekseiZhuvikin, “Selective Image Authentication usingShearletCoefficients Tolerant to JPEG Compression”, Page s: 681 – 688, IEEE 2017.

[4] Morteza Heidari1, Nader Karimi, and Shadrokh Samavi, “A Hybrid DCT-SVD Based Image Watermarking Algorithm”, Iranian Conference on Electrical Engineering (ICEE), IEEE 2016.

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