Security Implementation for Secret Data using Digital Watermarking & Encryption Technique

Reenu Rani[#1] & Neeraj[#2]
[1]Department of Computer Science & Engineering, PM College of Engineering Kami, Sonepat Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[2]Department of Computer Science & Engineering, PM College of Engineering Kami, Sonepat Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat

Received: January 06, 2019 Accepted: February 08, 2019

ABSTRACT: *Today digital communication has become an extremely important area of concern and mostly applications are internet based. Excessive use of internet for communication purpose increases the possibility of attacks. Hence security during communication has become a fundamental issue. Security of information depends on the privacy of its existence and confidentiality of its decoding methods. Digital data security can be achieved in two ways-encryption and data hiding. Cryptography technique distorts the information in such a way that it cannot be recognized. Steganography and Digital watermarking are the popular data hiding techniques. Steganography prevents suspecting the existence of data by inadvertent recipient but digital watermarking provides copyright protection by hiding legal information. In this paper, we suggest novel technique using digital image watermarking based on two techniques that are Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to hide the watermark image into original image. Also to enhance the security we apply encryption technique on the watermarked image so that watermark is available only to a legitimate user.*

Key Words*: Image Watermarking, DWT, SVD, Encryption & Decryption.*

I. INTRODUCTION

Digital watermarking [1] is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format.

Figure 1 below shows a typical digital watermarking system.

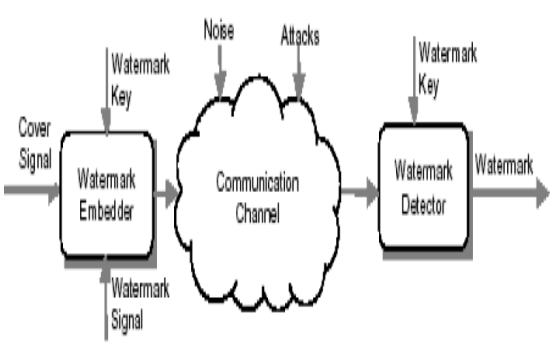

Figure 1: Digital Watermarking System

The digital watermarking system essentially consists of a watermark embedder and a watermark detector as shown in figure above. The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal.

An entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. The communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks [2].

Digital data security can be achieved in two ways-encryption and data hiding. Cryptography technique [3] distorts the information in such a way that it cannot be recognized. Steganography and Digital watermarking are the popular data hiding techniques. Steganography prevents suspecting the existence of data by inadvertent recipient but digital watermarking provides copyright protection by hiding legal information [4].

In this paper, we suggest novel technique using digital image watermarking based on two techniques that are Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to hide the watermark image into original image. Also to enhance the security we apply encryption technique on the watermarked image so that watermark is available only to a legitimate user.

II. CLASSIFICATION OF WATERMARK ALGORITHMS

There are different classifications of digital watermark as explained below [5][6].

A. According to characteristics/robustness

According to robustness feature digital watermarking is divided into following three categories:

1. Robust: Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark.

2. Fragile: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

3. Semi fragile: Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression.

B. According to attached media/host signal

According to host signal digital watermarking is divided into following five categories:

1. Image watermarking: This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.

2. Video watermarking: This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.

3. Audio watermarking: This application area is one of the most popular and hot issue due to internet music, MP3.

4. Text watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

5. Graphic watermarking: It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright.

C. According to perceptivity:

According to human perception digital watermarking is divided into following two categories:

1. Visible watermark: The watermark that is visible in the digital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture.

2. Invisible watermarking: There is technology available which can insert information into an image which cannot be seen, but can be interrogated with the right software. You can‘t prevent the theft of your images this way, but you can prove that the image that was stolen was yours, which is almost as good.

D. According to its purpose:

According to purpose of use digital watermarking is divided into following four categories:

1. Copyright protection watermarking: This means if the owner want others to see the mark of the image watermark, then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked.

2. Tampering tip watermarking: It protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats.

3. Anti-counterfeiting watermarking: It is added to the building process of the paper notes and can be detected after printing, scanning, and other processes.

4. Anonymous mark watermarking: It can hide important annotation of confidential data and restrict the illegal users to get confidential data.

E. According to watermark type:

According to watermark type digital watermarking is divided into following two categories:

1. Noise type: Noise type has pseudo noise, Gaussian random and chaotic sequences.

2. Image type: There are binary image, stamp, logo and label.

F. According to detection process:

According to detection process digital watermarking is divided into following three categories:

1. Visual watermarking: It needs the original data in the testing course, it has stronger robustness, but its application is limited.

2. Semi blind watermarking: It does not require an original media for detection.
3. Blind watermarking: It does not need original data, which has wide application field, but requires a higher watermark technology.

G. According to use of keys:
According to types of keys used for embedding & extraction digital watermarking is divided into following two categories:
1. Asymmetric watermarking: This is technique where different keys are used for embedding and detecting the watermark.
2. Symmetric watermarking: Here same keys are used for embedding and detecting the watermark.

H. According to domain:
Finally, based on processing-domain, watermark techniques can be divided into two categories [7][8]:
1. Spatial domain: A watermark technique based on the spatial domain, spread watermark data to be embedded in the pixel value. These approaches use minor changes in the pixel value intensity. The simplest example of the former techniques is to embed the watermark in the least significant bits of image pixels. In other words, significant portions of low frequency components of images should be modified in order to insert the watermark data in a reliable and robust way. As another example, an image is divided into the same size of blocks and a certain watermark data is added with the sub-blocks.
2. Transform domain: To have imperceptibility as well as robustness, adding of watermark is done in transform domain. In this method, transform coefficients are modified for embedding the watermark. Transform domain is also called frequency domain because values of frequency can be altered from their original. The most important techniques in transform domain are Discrete cosine transform (DCT) and Discrete Wavelet Transform (DWT) & Discrete Fourier transform **(**DFT).

III. PROPOSED WORK

Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. Nowadays, digital watermarking has many applications such s broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control, and file reconstruction. Digital Watermarking is a technique to insertion of data into digital multimedia, without affecting quality of the original multimedia. Digital watermarking technology plays an important role in preventing copyright violation as it allows to place an imperceptible or invisible watermark depending on the requirement in the multimedia data to detect malicious tampering of the multimedia or data identify the legitimate owner.
There are various techniques in implementing digital watermarking [9]. These techniques are commonly categorized in terms of working domain i.e. spatial domain or transform domain. In spatial domain, pixel luminance and chrominance values are modified to embed the watermark for example Least Significant Bit (LSB), correlation based and patchwork techniques. While in transform domain, the media content undergoes mathematical transformation before watermark embedding is done for example using Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).
In this paper, we suggest novel technique using digital image watermarking based on two techniques that are Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to hide the watermark image into original image. Also to enhance the security we apply encryption technique on the watermarked image so that watermark is available only to a legitimate user.
The following sections will explain the different methods used in our proposed work.

A. Discrete Wavelet Transform:
Discrete wavelet transform (DWT) of the image produces multi resolution representation of an image. The multi resolution representation provides a simple framework for interpreting the image information. The DWT analyses the signal at multiple resolution. DWT divides the image into high frequency quadrants and low frequency quadrants. The low frequency quadrant is again split into two more parts of high and low frequencies and this process is repeated until the signal has been entirely decomposed [10].
The single DWT transformed two dimensional image into four parts: one part is the low frequency of the original image, the top right contains horizontal details of the image, the one bottom left contains vertical details of the original image, the bottom right contains high frequency of the original image. The low frequency coefficients are more robust to embed watermark because it contains more information of the original image. The reconstruct of the original image from the decomposed image is performed by IDWT.
The digital wavelet transform are scalable in nature. DWT more frequently used in digital image watermarking because of its excellent

spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently.

B. Singular Value Decomposition (SVD)

The SVD is one of linear algebra tools. And, it is an approximation and factorization technique that effectively reduces any matrix into a smaller invertible matrix, where SVD of a rectangular matrix A is a decomposition of the form [10]:

$A(M*N) = U(M*M)S(M*N)V(N*N)$

Where *U* and *V* are orthogonal matrices and *S (sigma)* is a diagonal matrix. The columns of *U* are called the left singular vectors and the columns of *V* are called the right singular vectors and the diagonal elements of *S* are called the singular values (non-negative diagonal elements in decreasing order).

We use SVD to increase the quality and robustness of the watermark technique.

C. ENCRYPTION TECHNIQUE

A safe data exchange between source and target has always been one of the big challenges in data transmission. The challenge seems more serious whenever the confidentiality of transmitted data is higher. One of the important data in information transmission is digital images. Transmitted images can have military, trading, or even medical applications, but regardless of the field, the security and preventing impermissible access of images is indisputable.

With the growth of social networks, huge data such as audio files, video files, and images can easily be transmitted to the internet. Therefore it is necessary to protect them from impermissible access. One way of keeping secret data transmission secure is encryption. Encryption is the knowledge of changing message body or information by the help of a code key and an encryption algorithm so that only the person who knows keys and algorithm can extract the original information from encrypted information; and a person who does not know one or both cannot have access to them.

Encryption Algorithm is divided into two types, symmetrical and asymmetrical [11]. In symmetrical algorithm two sides of sender and receiver use the same key for encryption and decryption. In this case, data decryption and encryption are two reverse processes. In asymmetrical algorithm sender and receiver use the different keys for encryption and decryption. In this work we use symmetrical algorithm for encryption & decryption.

IV. IMPLEMENTATION RESULTS

Figure 2 below shows the original color image to be watermarked.

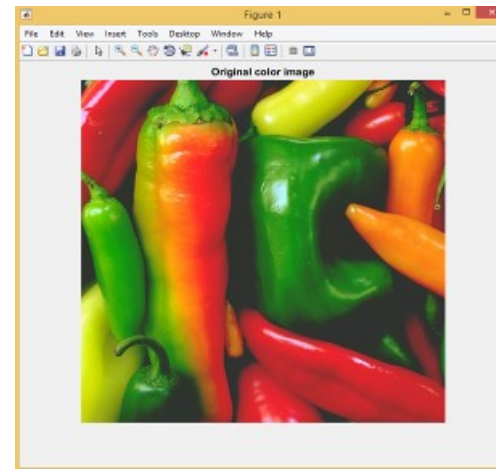

Figure 2: Original Color Image

Figure 3 below shows the original watermark image for embedding in cover object.

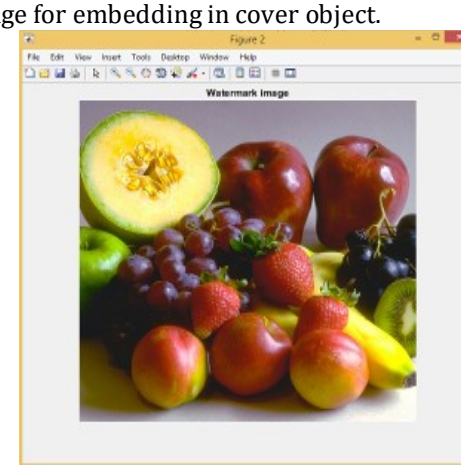

Figure 3: Watermarked image for embedding

Figure 4 below watermarked object i.e., object containing watermarked image without losing any quality.

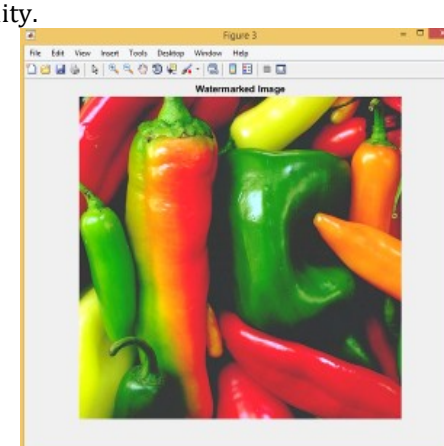

Figure 4: Watermarked object conatining watermark data

After embedding watermark object into cover object, we enhance security of watermarked object by encrypting this watermarked object using encryption technique. Figure 5 below shows the encrypted watermark object.

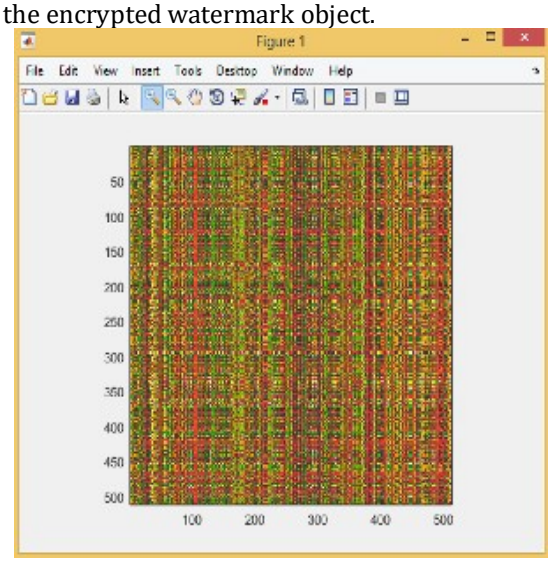

Figure 5: Encrypted watermarked object

V. CONCLUSION

The information which is being transmitted from one place to another is vulnerable to various types of active and passive attacks. Therefore, the security of the data and information is one of the most challenging aspects of computer communication in today' time. Cryptography, Steganography & watermarking are the process of hiding information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. There are various techniques in implementing digital watermarking. These techniques are commonly categorized in terms of working domain i.e. spatial domain or transform domain. In this thesis, we suggest novel technique using digital image watermarking based on two techniques that are Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to hide the watermark image into original image. Also to enhance the security we apply encryption technique on the watermarked image so that watermark is available only to a legitimate user.

REFERENCES

[1] Ramandeep Kaur, Amandeep Kaur, "Hiding Copyright Mark in Images using Watermarking Technique", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 10, October 2014

[2] Seitz, J. (2005), "Digital watermarking for digital media", IGI Global.

[3]. Prabhsimran Singh, Sukhmanjit Kaur, Sabia Singh , "Cryptography: An Art of Data Hiding", Prabhsimran et al, / International Journal of Computer and Communication System Engineering (IJCCSE), Vol. 2 (1), 2015, 117-120. ISSN: 2312-7694

[4] Chauhan Usha, Singh Rajeev Kumar, "Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016.

[5] Deepti Shukla, Nirupama Tiwari and Deepika Dubey, "Survey on Digital Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.1 (2016), pp.239-244.

[6] Jaishri Guru, Hemant Damecha, "Digital Watermarking Classification: A Survey", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014.

[7] Smita Pandey, Rohit Gupta, "A Comparative Analysis on Digital Watermarking with Techniques and Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016.

[8] Mahua Pal, "A Survey on Digital Watermarking and its Application", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[9] Madhuri Tonge, Praveen kumar Malviya, Anshu Gupta, "Implementation of Digital Watermarking Algorithm based on DWT and DCT", International Journal of Advanced Engineering and Global Technology Vol-2, Issue-1, January 2014

[10] Jay Prakash Pandey Gajendra Singh, "Digital Color Image Watermarking using DWT-SVD Techniques in YUV and RGB Color Spaces", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, January 2015.

[11]. Saranyak, Mohanapiyar, Udhayan J, "A Review on Symmetric Key Encryption Techniques in Cryptography". International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014.