An Efficient Technique of Information Hiding using Hybrid Compression-Encryption with LSB Watermarking

Sonali Jaiswal, Apurva Saxena

Abstract— Watermarking is a new way of hiding secrete information so that the information is not accessible by other users. Since various techniques are implemented for the security of these secrete messages such as using spread spectrum technique. But the technique implemented so far is not efficient in terms of bit error rate and watermark signal strength. Hence a new and efficient technique is implemented using Hybrid Encryption-Compression based watermarking for the secrete hiding of information. The proposed methodology implemented here provides efficient results as compared to other existing techniques implemented for Watermarking.

Index Terms— Minimum 7 keywords

1 INTRODUCTION

he increasing use of Internet has permitted the consumers to Twithout problems right of entry, allocate, influence, and dispense the digital media data, and digital media has extremely transformed our daily life for the period of the past decade. This propagation of digital media data generates a scientific riot to the entertainment and media industries, brings innovative knowledge to consumers, and establishes innovative Internet ideas. On the other hand, the enormous production and use of digital media also masquerade innovative disputes to the exclusive rights industries and increase significant problems of defensive rational assets of digital media, in view of the fact that contemporary media sharing formulates unauthorized copying and illegal allocation of the digital media much easier.

In the digital watermarking technology, a specific signal is embedded into the host media content without significantly degrading the perceptual quality of the original media data, and the embedded information can later be removed for wanted intentions. In view of the fact that this embedded watermark signal is usually not perceptible, digital watermarking could make available post-delivery protection for the digital substance. Digital watermarking has numerous applications, and one essential application is data hiding method. Digital data hiding [1], where the embedded hidden message should be decoded accurately at the receiver side and such hidden information can be used to serve covert statements, facilitate authenticating the dependability of the digital media information, recognizing the original resource, and make possible the investigation on illegal usages and copyright violations.

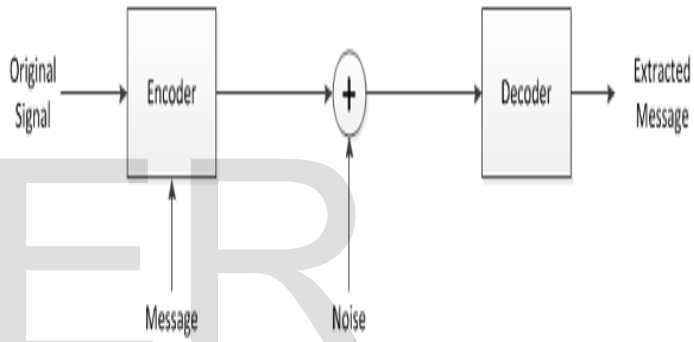

Figure 1: A Digital Data Hiding System.

2 TRADITIONAL EMBEDDING SCHEMES FOR DATA HIDING

Wherever each digital data hiding system should fulfill some requirements: the embedded watermark should be invisible, significance that the perceptual feature of the unique content should not be degraded due to watermarking. For some applications (e.g., the embedded message should be extracted accurately even after unauthorized distortions), robustness is important. Payload is another concern which arises in the applications where the number of embedded bits should be far above the ground. Protection of data is also a significant apprehension in data hiding, which implies that unauthorized party should not be able to reveal the hidden message, the extracted hidden information are compared with the original information in order to determine whether they are the identical. Most important data hiding methods used heuristic algorithms based on simple image processing exploitations. Transient moment in time, further difficult watermarking algorithms were proposed and used in different types of media data such as audio and video. Although many embedding schemes have been recommended, they may well

be generally classified into two groups: spread spectrum and quantization based methods.

Probably the first milestone in data hiding using watermarking was accomplished by Cox et al. [2] where they proposed Spread Spectrum (SS) method. In consequence [2] two versions of SS were suggested. The initial one is additive Spread Spectrum SS in which the watermark is spread over the host signal consistently. The subsequent one is the Multiplicative Spread Spectrum (MSS) which spreads the watermark according to the host substance. Figure 1.2 illustrates the SS embedding method where the dashed line shows that it is possible to add the watermark depending (MSS scheme) or without depending (additive SS scheme) on the content.

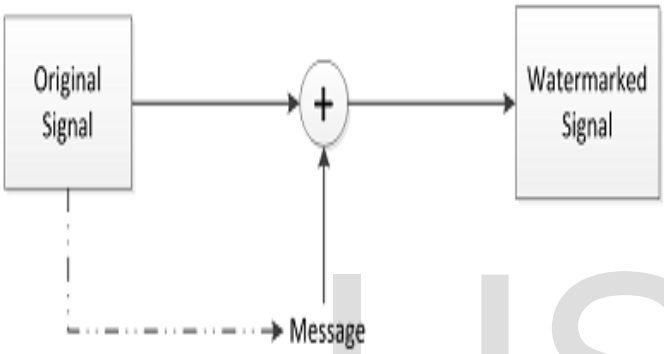

Figure 1.2: An illustration of spread spectrum-based embedding schemes.

In both schemes, in order to increase the safety measures, a top secret signature code for increasing the hidden message bits is used. SS schemes generally have huge strength. Hidden messages embedded underneath these methods could robustly resist against lossy compressions and many other types of distortions and attacks. In spite of their great robustness against standard signal processing operations and manipulations, the main drawback of SS-based schemes is the host interference effect. Since in the SS schemes the host signal itself acts like a noise source at the decoder side and because of the fact that the watermark has comparatively minute authority, the host indication requires a large intrusion effect which causes a serious degradation of the decoding performance. To reduce the interference effect of the host signal, Malvar and Florencio proposed the Improved Spread Spectrum (ISS) scheme [3] by exploiting the side information at the encoder side. Their result brought the hope of having a robust embedding scheme with good decoding concert. An additional imperative landmark in embedding methods was presented by Chen and Wornell [4] where they introduced a new class of embedding scheme called Quantization Index Modulation (QIM). Spread Transform Dither Modulation (STDM), an additional distinction of the original QIM, which combines the spread spectrum and quantization proposal was proposed in their work as well [4]. The QIM approach could improve the decoding performance greatly by removing the interference effect of the host signal due to its quantization embedding life. On the other hand, it experiences from understanding to scaling and lacking of content based embedding. Its sensitivity to scaling causes drastically degradation of its performance and lack of content based embedding makes it susceptible to observable watermark. Although some attempts have been completed to tackle these deficiencies [5, 6], more efforts are still needed for QIM to achieve a scheme which is robust against all of these problems. At the same time as reflexive detection-only of the attendance of embedded data is being intensively investigated in the past few times [7], active hidden data extraction is a comparatively new subdivision of research. In blind extraction of Spread Spectrum SS embedded data, the unknown host acts as a source of interference/disturbance to the data to be get bettered and in a technique the difficulty equivalents blind signal separation (BSS) applications as they arise in the fields of array processing, biomedical signal processing, and code-division multiple-access (CDMA) communication systems [8].

3 Literature Survey

In this paper, spread spectrum schemes [9] represent an early type of embedding technique. It appends a progression of pseudo-random indications into the host signals to form the watermarked data. According to how the watermark is added into the host contented, the spread spectrum methods can be additional subdivided into the additive and multiplicative spread spectrum i.e. ASS and MSS methods. The signals are frequently embedded into the perceptually significant components of the host image to achieve a balance of perceptual quality and robustness. At the detector, the original image should be available to cancel the watermarked image to extract the embedded signals. The extracted signals are then show a relationship with a predefined pattern for substantiation. The detection that necessitates the unique data is called private detection.

In this paper [10], author has to find a problem of blindly extracting unknown messages hidden in image hosts via multi-carrier/signature spread-spectrum embedding. In this proposed work author has to guess that the original host and the embedding carriers are offered. The extraction algorithm used to extract the hidden data from digital media and the proposed algorithm is a low complexity algorithm and it attains the probability of error recovery equals to known host and embedding carriers. The original host or the embedding carriers are assumed offered. Here they executed a low complexity multi-carrier iterative simplified least-squares (M-IGLS) core algorithm. Investigational cost demonstrated that M-IGLS can accomplish probability of error relatively close to what may be achieved with known embedding signatures and known original host autocorrelation matrix and presents itself as an efficient countermeasure to traditional SS data embedding or data hiding. The accomplishment of M-IGLS can achieve probabil-

ity of error to a certain extent secure to what possibly makes with known embedding signatures and known original host autocorrelation matrix and presents itself as efficient and well-organized countermeasure to conventional SS steganography.

In this paper [11], author tries to develop a new multicarrier iterative generalized least squares (M-IGLS) algorithm for SS hidden data extraction that, to the most excellent of the authors' acquaintance, become visible for the first time in the broad communication theory and techniques writing. To improve reinforcement arrangement, particularly for minute hidden messages that pretend to be the furthermost dispute, tentative studies point toward that a small amount of self-sufficient M-IGLS reinitializations and implementations on the host can show the way to hidden data recovery with probability of error close to what may be attained with known embedding carriers and known original host autocorrelation matrix. The reasons of enlarged algorithm are positively not highest importance to offensive steganographic concealed communications by improving the secret embedded messages. Since the delivery services are also mutually approximated with the embedded data, the extended method can also be used for entire message elimination or tampering attack as well by re-inserting a manufactured message in place of the original. From the contradictory data embedding move toward, the comprehensive algorithm can be amusement as an implement to experiment security strength of SS data hiding schemes.

Tung-Hsiang Liu and Long-Wen Chang [12] has proposed a simple data hiding technique for binary images.The proposed technique embeds make safe data at the edge portion of host binary image data. The Distance matrix method is utilized to discover the edge pixels of host binary image. After that the Weight mechanism is utilized to think about the connectivity of the region approximately unpredictable pixels for choosing the large amount appropriate one. For the safety measures and excellence thought, a random number generator is making use of to allocate the embedding data into the taken as a whole image data. This technique not only embeds huge quantity of data into host binary image but also can sustain image quality.

M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco & A. Neri [13] has proposed a no-reference video quality metric that blindly approximations the excellence of a video. They had used Block based Spread Spectrum embedding technique to introduce a easily broken scratch into perceptually significant neighborhoods of the video frames. They used a set of perceptual characteristics to differentiate the perceptual meaning of a region that are Motion, Contrast and Color. The mark is taken out from the perceptually significant neighborhoods of the decoded video on receiver side. Then a feature determine of the video is get hold of by computing the degradation of the removed mark. So, in this approach quality of a compressed video is approximation by using simple embedding method on perceptually significant neighborhoods of the video frame.

3 PROPOSED METHODOLOGY

1. Take an input image and a secrete image.
2. Choose alpha value which denoted watermark signal strength factor in spread spectrum algorithm, here in our work we assume alpha=5;
3. Calculate DWT of the original image which is used for the transformation of the image to be embedded.
4. Calculate total number of pixels of the original image and watermark image.
5. Calculate aj=bj where ir <=j < (i+1) r.
6. Calculate watermark signal as wj=alpha*aj*pj, where pj= {+1,-1}.
7. Now we will find the kernel of the image by taking kernel size 31 and by taking the level of the kernel size as 3 we will find the kernel image of the original image by calculating kernel image = (1/(2*pi*s^2))*exp(-((X-m).^2 + (Y-m).^2)/(2*s^2));
8. This watermark signal is then embedded with the kernel image to get the final watermark image.

SPREAD SPECTRUM WATERMARKING

The embedding process is carried out by first generating the watermark signal W by using watermark information bits, chip rate and PN sequence. The watermark information bits

$$a_j = b_i, \quad ir \leq j < (i+1)r.$$ ives

The sequence aj is then multiplied by alpha>0 and P. The wa-

$$w_j = \alpha a_j p_j$$ vj}, where

Where, pj={1,-1} The watermark signal generated is added to

$$\boldsymbol{C}_W = \boldsymbol{C} + \boldsymbol{W} = c_{w_i} = c_i + w_i \quad \forall i = 0, 1,$$

The encrypted value of M2 denoted by C2 is

$$c_{2_i} = (m_{2_i} + k_{2_i}) \bmod 255 \ \forall i = 0, 1, \ldots, I$$

KERNEL BASED IMAGE DETECTION

1. ksize_image = 31;

It is the kernel size that we want to make the sie of the kernel.

2. kernel = zeros(ksize_image);

Whatever the size of the kernel make the pixel value of all zeros.

3. s = 3;

It is the segmented part from the kernel image.

4. [X, Y] = meshgrid(1:ksize_image);

Generate X and Y arrays for 3-D plots from 1 to the size of the kernel and stores rows and columns in X and Y.

5. kernel_image = (1/(2*pi*s^2))*exp(-((X-m).^2 + (Y-m).^2)/(2*s^2));

Now calculate the original kernel by reducing the total size and the size of the kernel taken.

Kernel image is used for the embedding of kernel region in the image

the total effect of blurriness is pointed out so that it will be helpful for the detection of embedding part of the image.

LSB ALGORITHM

The least significant bit (LSB) technique is used to embed information in a cover image. The LSB technique is that

inside of a cover image, pixels are changed by bits of the secret message. These changes cannot be perceived by the human visibility system However; a passive attacker can easily extract the changed bits, since it has performed very simple operation.

After the secret data gets embedded or hidden in the cover image, the original cover image will get modification to some extent with respect to the length of the secret data. At the receiving end we are not able to get back the original cover image since our traditional LSB is not providing reversibility. Reversible feature is a process of getting back the cover image from the watermarked or embedded image at the extraction phase. After getting the watermarked image, we need to create a matrix initialized with zeros, whose dimension is equal to the watermarked image. By XORing each and every pixel of both the original and watermarked image, the result will be stored in the corresponding positions in the newly created matrix. This matrix will also be sent to the extraction phase along with the watermarked image. During extraction the value of the newly created matrix will be checked. If it is 1, then watermarked image's s LSB of each pixel must be changed, else vice versa. Finally we could get back to the original cover image.

3 Result Analysis

The table show below is the result analysis and comparison of the proposed methodology on various parameters for different images.

Image	No. of Colors	Mean square Error	NCC	NAE
Woman	254 Experimental & simulation result ……	1.6640e+004	4.3038e-004	1.0005
Lena	239	1.5703e+004	7.2774e-004	1.0004
Satellite	256	9.6603e+003	-0.0016	1.0042

Table 1. Result Analysis of the Existing Work

The Table shown below is the analysis and comparison of existing and proposed work on the basis of CPU Time and PSNR and Payload capacity.

Parameters	Existing Work	Proposed Work
CPU Time	4.493	0.218
PSNR	34.1514 db	33.396 db
Payload Capacity	800	683

Table 2. Comparison of Existing & Proposed Work

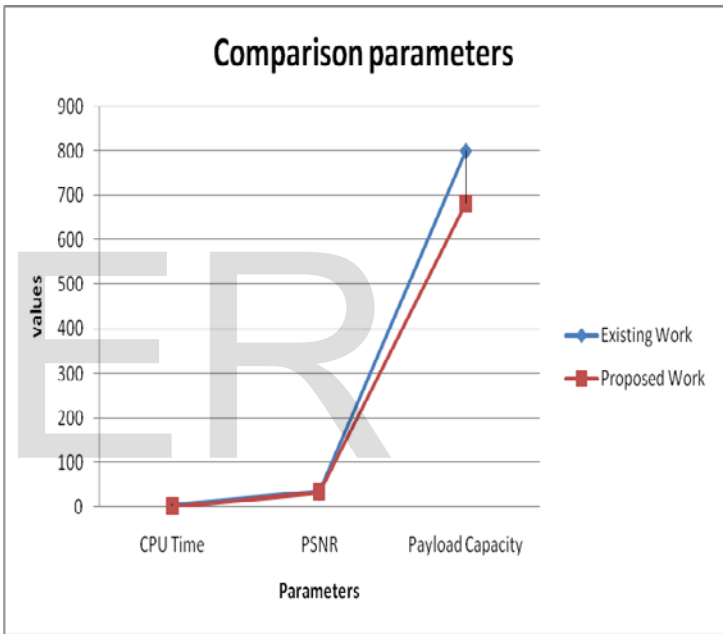

Figure 3. Comparison of Existing & Proposed Work

3 Conclusion

The digital revolution, the explosion of communication networks, and the increasingly growing passion of the general public for new information technologies lead to exponential growth of multimedia document traffic. The digital watermarking is a technique of authenticating the user, here the methods that are applied increases the efficiency of the security mechanism. Here in this paper we enhance the security of the watermarked images using the combinatorial method of compression and encryption. The proposed technique here provides best results as compared to the existing techniques. Our scheme also preserves the confidentiality of content as the embedding is done on encrypted data. The homomorphic property of the cryptosystem is exploited, which allows us to detect the watermark after decryption and control the image quality as well.

REFERENCES

[1] F. Y. Shih. Digital watermarking and steganography: fundamentals and techniques. CRC Press, 2008.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shanon. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process, 6(12):1673–1687, 1997

[3] H. S.Malvar and D. A. Florencio. Improved spread spectrum: A new modulation technique for robust watermarking. IEEE Trans. Signal Process, 51(4):898–905, 2003.

[4] B. Chen and G. Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Trans. Inf. Theory, 47(4):1423–1443, 2001.

[5] N. Khademi-Kalantari and S. M. Ahadi. A logarithmic quantization index modulation for perceptually better data hiding. IEEE Trans. Signal Process. 19(6):1504–1517, 2010.

[6] F. Perez-Gonzales, C. Mosquera, M. Barni, and A. Abrardo. Rational dither modulation: A high-rate data-hiding method robust to gain attacks. IEEE Trans. Signal Process, 53(10):3960–3975, 2005.

[7] G. Gul and F. Kurugollu, "SVD-based universal spatial domain image steganalysis," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 349–353, Jun. 2010.

[8] T. Li andN.D. Sidiropoulos, "Blind digital signal separation using successive interference cancellation iterative least squares," IEEE Trans. Signal Process., vol. 48, no. 11, pp. 3146–3152, Nov. 2000.

[9] I. J. Cox, J. Killian, F. T. Leighton, and T. Shanmoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[10] K.Bharath Kumar, Bhaludra Raveendranadh Singh, "Hiding and Extracting Secret Data from Digital Media" International Journal of Computer Trends and Technology (IJCTT) – volume 16 number 2 – Oct 2014

[11] Ming Li, Michel K. Kulhandjian, "Extracting Spread-Spectrum Hidden Data From Digital Media" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013.

[12] Tung-Hsiang Liu and Long-Wen Chang, "An Adaptive Data Hiding Technique for Binary Images", Proc. IEEE 17th Int.Conf. On Pattern Recognition (ICPR'04), 2004.

[1] M. Carli , M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A. Neri, "QUALITY ASSESSMENT USING DATA HID-ING ON PERCEPTUALLY IMPORTANT" IEEE AREAS0-7803-9134, 2005.