International Journal of Engineering Sciences Paradigms and Researches [Volume 47, Issue: Special), March 2018]
www.ijesonline.com ISSN (Online): 2319-6564

AES and DWT based CRYPTO-STEGO Method

Ratiranjan Moharana
Raajdhani Engineering College, Bhubaneswar
ratiranjan moharana@rec.ac.in

Abstract

The method that will encrypt the message and conceal it within the altered image is covered in this paper. Both the imperceptibility and the PSNR value will increase as a result. The cover image's DWT will be used to breakdown the image. The AES method is used to encrypt the secret message. The encrypted message is then concealed within the picture on the cover. The diagonal detailed area and the approximation portion of the cover image conceal the encrypted message. The MSBs from the R, G, and B blocks are gathered and given a decimal value. If the MSB has two or more 1s in the HH portion.

Keywords: *Cryptography, Stegnography, AES, DWT.*

1. Introduction

The word Steganography is of Greek source and means "enclosed or hidden writing". Data hiding should be used as concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden [1]. Steganography is implemented in different fields such as military and Industrial applications. By using lossless steganography techniques messages can be sent and received securely [2]. Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. *Cryptography* is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, *cryptanalysis* is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called *attackers*. *Cryptology* embraces both cryptography and cryptanalysis [3].

2. Combined Crypto-Steganography

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key[5]. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data

transmission over an open channel. A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 1.6 [6].

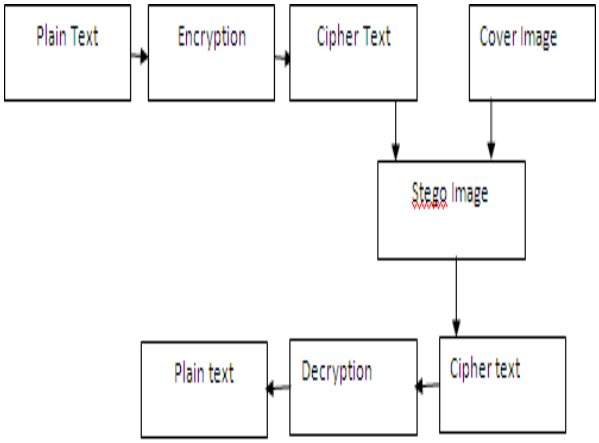

Figure 1: Combination of Steganography and Cryptography.

In figure 1, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types:

Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

Secret Key steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach.The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

Public Key Steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

3. DWT

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. A wavelet series is a representation of a square-integral function by a certain ortho-normal series generated by a wavelet. Furthermore, the properties of wavelet could decompose original signal into wavelet transform coefficients which contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the sub bands of the cover image [4].

Advantages of DWT

1. No need to divide the input coding into non-overlapping 2-D blocks, it has higher compression ratios avoid blocking artifacts.
2. Allows good localization both in time and spatial frequency domain.
3. Transformation of the whole image introduces inherent scaling
4. Better identification of which data is relevant to human perception higher compression ratio .
5. Higher flexibility: Wavelet function can be freely chosen.

Disadvantages of DWT

1. The cost of computing DWT as compared to DCT may be higher.
2. The use of larger DWT basis functions or wavelet filters produces blurring and ringing noise near edge regions in images or video frames.
3. Longer compression time.

4. AES Cryptography

Encryption is always going to be necessary for maintaining privacy in our personal communications. In fact it was created for that exact reason. However people are always finding new ways of “breaking”

encryption and therefore leaving these communications open to being read or possibly tampered with by a third party. In 1997 The Unites States National Institute of Standards and Technology (NIST) asked the public, including academics and professionals, to submit new cryptography algorithms as possible candidates to become the new Advanced Encryption Standard (AES). The previous standard called the Data Encryption Standard (DES) was in need of replacement by a new algorithm which was to be used throughout the US government to encrypt sensitive (but not classified) information. There were 3 main candidates for the new standard namely, Rijndael, Serpent, 2fish, RC6 and MARS. In November 2001 Rijndael was chosen as the new AES algorithm. Rijndael can encrypt using 128, 192 and 256 bit cipher keys which are applied, using the algorithm, to data blocks of 128bits to perform the required transformation [7].

The AES (advanced encryption standard) [8, 9] is an encryption standard as a symmetric block cipher. It was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26,2001. The Rijndael algorithm was developed by Joan Daemen of Proton World International and Vincent Fijmen of Katholieke University at Leuven. The AES consists of mainly two units which are Data processing unit and the other one is Key Expansion unit. The Data processing units have four main modules or transformations in which sub byte transform, shift rows, mix column and add round key are involved and the Key Expansion unit generate the round key for the next round.

5. Proposed Work

In this system the message will be encrypted and the encrypted message will be hided in to the transformed image. This will improve the PSNR value and the imperceptibility will also get improved. The cover image will be decomposed by taking the DWT of the cover image. The secret message is encrypted by using the AES algorithm. Then the encrypted message is hided in to the cover image. The encrypted message is hided in to the approximation part and the diagonal detailed part of the cover image. The MSB of the R, G and the B block is collected and converted in to a decimal value. If MSB contains two or more 1's in HH part or the MSB contains two or more 0's in the LL part then the MSB is ignored. It means no message will be hided in such MSB. Otherwise if the bit at the decimal position in the B component is similar to the message bit then the LSB of the pixel will remain same otherwise complemented. The process is repeated until the whole message is stored in to the cover image. Then the IDWT is used to get the cover image in to the time domain. This is the resultant image. The resultant image is visually same as the original image. The process hides the message in to the transformed domain of the image, this increases the imperceptibility of the image. The imperceptibility can be verified by the PSNR value. This process can be easily understood by the following algorithms. Firstly the embedding algorithm explains the process of hiding the message in to the image then the extraction explains the process to extract the message from the image.

Embedding Algorithm

1. Get the cover image.
2. Take DWT of the cover image to decompose the image in 4 parts.
3. Collect the MSB bits from a pixel (Red, Green, Blue color component)
4. Get the Original message
5. Encrypt this original message with AES encryption technique.
6. Convert the AES cipher into binary number say bm
7. for i=1:length(bm) repeat
8. From the MSBs, if it contains two bits 1 for LL or if it contains two bits 0 for HH, select this pixel for hiding message bit. Otherwise, skip this pixel. Convert MSB into decimal number say DM.
9. If DM=0 for the HH part only embed the message bit into the Blue color component of the pixel.
10. For LL or other value of DM: a. Check DM bit position of the Blue color component with message bit
    a. If it matches then change the LSB of Blue color component with 1(indicate status true)
    b. If it does not match with message bit then change the LSB of Blue color component with 0(indicate status false).

    End for
11. Take IDWT of the image.

Extracting Algorithm

1. Get the Stego image.
2. Take DWT of the Stego image
3. Collect the MSB bits from a pixel (Red, Green, Blue color component).
4. From the MSBs, for LL if it contains two bits 1 and for the HH or if it contains two bits 0, select this pixel for hiding message bit. Otherwise, skip this pixel.
5. Convert MSB into decimal number say DM.
6. If DM=0 only get the cipher binary from Blue component of the pixel.
7. If DM>0, Check the LSB (Status bit) whether it is 0 or 1.
8. If the LSB equals to 0, then collect the cipher binary by toggling the DM bit of the Blue component of the pixel.
9. If the LSB equals to 1, then collect the cipher binary as the DM bit of the Blue component of the pixel.
10. Apply AES to decrypt the original message from cipher text.

Table 1: Comparison of PSNR over Various Images with Same Message

IMAGE NAME	EXISTING	PROPOSED
Lena	38.71	49.09
1.jpg	44.99	55.55
2.jpg	55.5575	94.98

Table 2: Comparison of MSE over Various Images with Same Message

Image Name	EXISTING	PROPOSED
Lena	8.73	0.8002
1.jpg	2.0573	0.1809
2.jpg	0.1809	.000020616

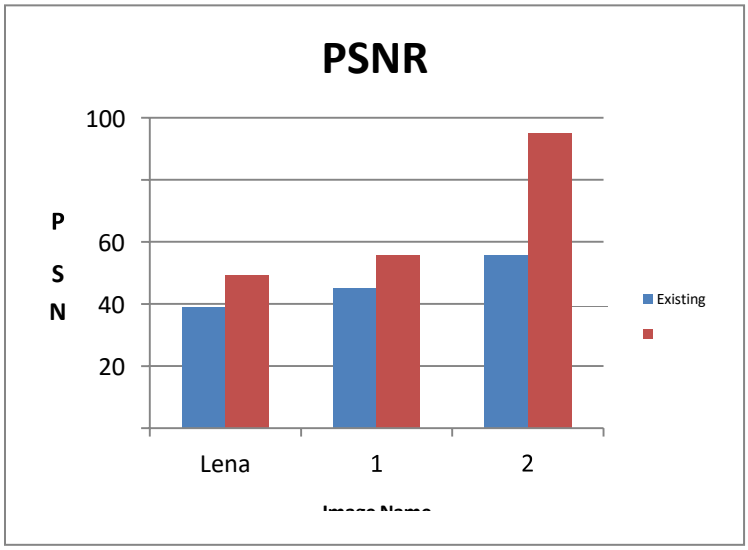

Figure 2: Comparison of PSNR using Same Message

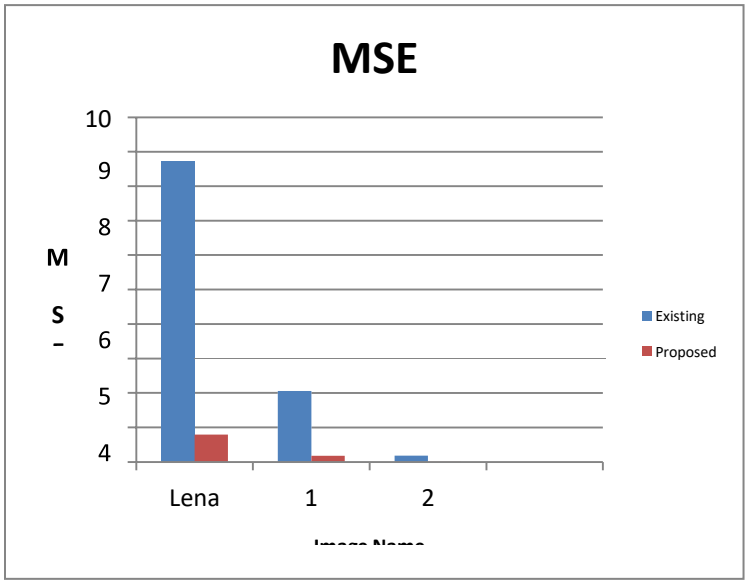

Figure 3: Comparison of MSE using Same Message

The comparison of the PSNR and MSE values for the different images with same message is shown in above figures. The comparison shows the decrease in the MSE and increase in the PSNR value. The

increase in the PSNR value represent in increase in imperceptibility.

Table 3: Comparison of PSNR over Same Image with Different Messages

Message	EXISTING	PROPOSED
Hellooiu	44.99	55.55
hellooiu hellooiu	42.0706	50.55
hellooiu hellooiu hellooiu	40.2515	47.05

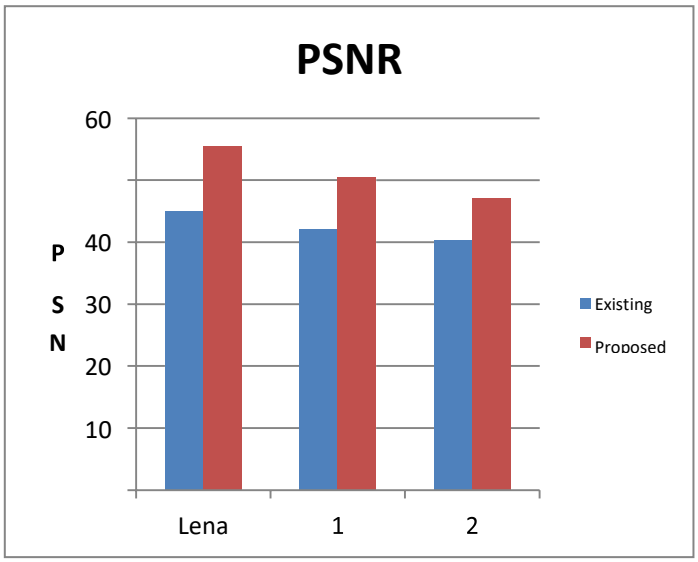

Figure 4: Comparison of PSNR using Different Message

Table 4: Comparison of MSE over Same Image with different messages

Message	EXISTING	PROPOSED
Hellooiu	2.0573	0.1809
Hellooiuhellooiu	4.0366	0.5727
hellooiuhellooiuhellooiu	6.1366	1.2806

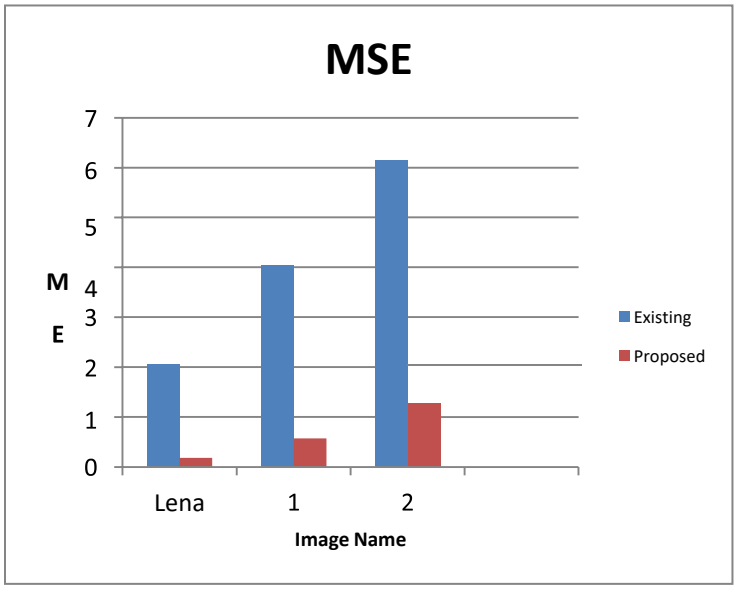

Figure 5: Comparison of MSE using Different Message

6. Conclusion

The comparison of the PSNR and MSE values for the same images with different message is shown in above figures. The comparison shows the decrease in the MSE and increase in the PSNR value.

imperceptibility. The security as well as the imperceptibility is increased in the present technique.

In future the technique can be extended by using neural networks or fuzzy. The technique can also be extended by using key authenticity.

References

[1] Anderson R.J. and Petitcolas F.A.P., "On the Limits of steganography," J. Selected Areas in Comm., vol. 16, no.4, 1998, pp. 474–481.
[2] K. Su, D. Kundur, and D. Hatzinakos, "Statistical Invisibility For Collusion-Resistant Digital Video Watermarking," IEEE Trans. Multimedia, 2005,(7)1:43-51.
[3] http://fisher.osu.edu/~muhanna.1/pdf/crypto.pdf.
[4] Patel, Komal D., and Sonal Belani. "Image Encryption Using Different Techniques: A Review." International Journal of Emerging Technology and Advanced Engineering 1.1 (2011): 30-34.
[5] "Encryption and Decryption techniques", (2009) Security Framework in HDD.
[6] A. Joseph Raphael "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.
[7] Christopher Feldwick "Implementation and Analysis of the Advanced Encryption Standard (AES) Algorithm in Different Memory Configurations", BSc (Hons) in Mathematics and Computing May 2005.
[8] Saini, Vedkiran, Parvinder Bangar, and Harjeet Singh Chauhan. "Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application.", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume2, Issue-6, April 2014.
[9] Qin, Hui, Tsutomu Sasao, and Yukihiro Iguchi. "An FPGA Design Of AES Encryption Circuit With 128-Bit Keys." Proceedings of the 15th ACM Great Lakes symposium on VLSI. ACM, 2005.