ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Data Hiding In Encrypted Images by Reversible Image Transformation

[1] R.Sivaranjani, [2] R.Kanimozhi, [3] A.Suhasini
[1] M.E Scholar, [2] Ph.d Scholar, [3] Associate professor
[1][2][3] Annamalai University,Chidambaram.

***Abstract* - An information concealing is that the technique by that some information is hidden into a cover media. It will be exhausted audio, video, image, text and film. The mistreatment of Watermark within the encrypted image will satisfy completely different wants on image quality and enormous embedding capability severally. The user encrypts the first compressed image mistreatment associate the encoding key. With associate encrypted image containing further information, and transfer the encrypted information onto cloud storage. Outsourced information to the cloud, it is important to shield the privacy of knowledge change the cloud server to simply manage the information. The user will decipher then reveals the information hidden into cover media at an equivalent time with none loss.**

***Keywords:*--- information concealing, Image encryption, Image decryption, cloud storage.**

I. INTRODUCTION

Data security primarily suggests that protection of information from unauthorized users or hackers and providing high security to stop data modification. This space (of information or of knowledge) security has gained additional attention over the recent amount of your time thanks to the large increase in data transfer rate over the net. So as to enhance the safety options in information transfers over the net, several techniques are developed like: Cryptography, Steganography. Whereas, Cryptography could be a methodology to hide data by encrypting it to cipher texts associated sending it to the supposed receiver mistreatment an unknown key, Steganography provides additional security by concealing the cipher text into a apparently invisible image or alternative formats.

Security is very important side in day to day life. So, everybody used varied ways in which for security purpose. The sender uses the password for his or her security. Digital pictures have exaggerated speedily on the net. Image security becomes more and more vital for several applications, e.g., confidential transmission, video police work, military and medical applications.
The protection of this multimedia system information will be through with coding or information concealing algorithms within the coding sort.

To protection through secret writing there square measure many strategies to write in code binary pictures or grey level pictures and second kind the protection on digital watermarking or information concealing, geared toward on the embedding a message into the information.

These two technologies is used complementary and reciprocally independent. This method is to write in code a picture for secure image transmission. In different approach the digital signature of the initial image is another to the encoded version of the initial image.

The cryptography of the image is finished exploitation Associate in nursing acceptable error management code. At the receiver finish, once the cryptography of the image, the digital signature is wont to verify the credibleness of the image. The secret writing and watermarking algorithms are utilized in digital pictures.

In every sample of a canopy signal is encrypted by a public-key mechanism and a homomorphic property of secret writing is exploited to plant some further information into the encrypted signal. However the information quantity of encrypted signal is considerably distended and also the computation complexness is high. Also, the information embedding is not reversible.

This work proposes a unique reversible information concealing theme for encrypted images, these is created from image secret writing, information embedding and data-extraction/image-recovery phases. The information of original cover square measure entirely encrypted, and also the further message is embedded by modifying a locality of encrypted information. At receiver aspect, with the help of spatial correlation in natural image, the embedded information square measure with success extracted whereas the initial image is utterly recovered.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

IMPLEMENTATION

Image improvement

Apply Watermark to a picture it will be visible signature embedded within a picture to point out credibleness or proof to possession. Discourage unauthorized repetition and distribution of pictures over the web. Guarantee a digital image has not been altered computer code is wont to rummage around for a particular watermark algorithmic rule to create text visible.

Applying Image Watermark:

An initially changing the particular watermark to a binary image (a inexperienced picture element signifies a 1 and a black picture element signifies a zero within the mark), then pressing this image to JPEG format. The digital watermarking may be a field of information concealing that hide the crucial information within the original information for defense illicit duplication and distribution of multimedia system data. Applying the watermark in image and checking the text visible.

The watermark embedding algorithm could be described as follows:

$$X = S\,(1+ \alpha W)$$

Where S is the original host signal, X is the watermarked signal, and W is the watermark consisting of a random, mathematician distributed sequence α is a scaling issue, that the authors counsel to set to zero. And one to give a smart trade-off between physical property and strength.

Image Compression

Image compression is minimizing the scale in bytes of a graphics file while not degrading the standard of the image to an unacceptable level. The reduction in file size permits additional pictures to be keep in a very given quantity of disk or memory area. It additionally reduces the time needed for pictures to be sent over cloud storage. Compression the image to optimize the scale and store in cloud server uses DCT algorithm.

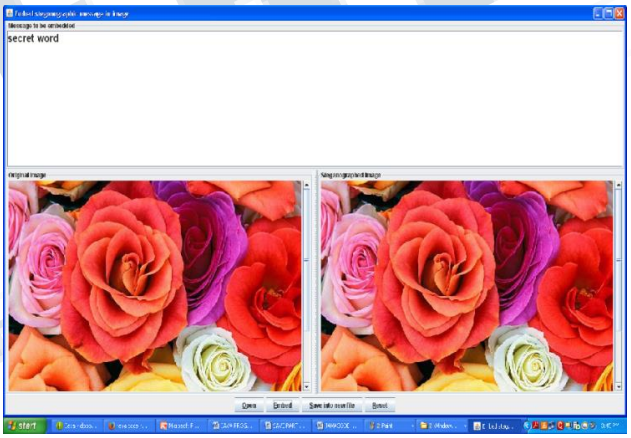
Compression Metrics:

Two of the metrics accustomed compare the assorted compression techniques area unit the Mean sq. Error (MSE) and therefore the Peak Signal to Noise quantitative relation (PSNR). The MSE is that the additive square error between the compressed and therefore the original image, whereas PSNR may be a live of the height error. The mathematical formulae for the 2 are where I(x,y) is the original image, I'(x,y) is the approximated version (which is really the process of

$$SE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

PSNR = 20 * log10 (255 / sqrt(MSE))

decompressed image) and M,N as the size of the pictures. A lower worth for MSE means that lesser error, and as seen from the inverse relation between the MSE and PSNR, this interprets to a high worth of PSNR. Logically, a higher value of PSNR is sweet as a result of it implies that the quantitative relation of Signal to Noise is higher. Here, the 'signal' is that the original image, and therefore the 'noise' is that the error in reconstruction. We discover a compression theme having a lower MSE (and a high PSNR), we will be able to acknowledge that it's a more robust one.



Data Embedding

Applying steganography rule to cover the text in image. Steganography is that the art of concealing the actual fact that communication is going down, by concealing data in alternative data. the key message is embedded within the lined media on that stego-function is applied in conjunction with stego-key or watchword to create a stego-object. These pictures as one amongst the popular media to cover the knowledge owing to their high capability and low impact on the visibility. We are able to use the common image format of pictures like GIF, BMP ,JPEG, etc.

The data or data embedding technique is that during which great amount of knowledge will be embedded into the original image. It permits the user to decide on the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

suitable the image that is best fitted to cover image and fewer prone to the steganalysis attacks. The information is made from that the best cover pictures as extracted. For embedding procedure to initial choose the suitable image from the information is understood as a canopy image. The purpose of the projected system is to produce a robust steganographic technique that accomplishes embedding capability and high security whereas preserve physical property and quality of the image.

Image Encryption

In cryptography, coding is that the method of encryption a message or data in such the simplest way that solely approved parties will access it, coding does not itself forestall interference, however denies the intelligible content to a would-be attack aircraft. In Associate in nursing coding theme, the meant data or message, observed as plaintext, is encrypted victimisation Associate in nursing encryption rule – a cipher – generating cipher text which will solely be scan if decrypted. Here we have a tendency to uses DES rule to encode the key for security.

Image Decryption

The plaintext is encrypted victimisation Associate in nursing coding DES rule – a cipher – generating cipher text which will solely be scan if decrypted. Associate in nursing coding theme sometimes uses a pseudo-random coding key generated by Associate in nursing rule. It is in essence attainable to rewrite the message while not possessing the key. A licensed recipient will simply rewrite the message with the key provided by the mastermind to recipients however to not unauthorized users. In receiver finish uses the rewrite the key victimisation DES rule.

It is a reverse method of Image coding. During this technique encrypted image is taken into account as input for DES rule structure for cryptography. Encrypted image is split once more into component blocks that as same as DES rule block length. Primarily operate blocks of 64-bit size ar entered.

Then same secrecy key that's cryptography key used for method of coding that one is employed for coding. Here we have a tendency to follow a reverse ordered procedure of coding. once completion of cryptography, obtained output is taken into account as decrypted image, it follows the same characteristics of original image.

Data Extracting

The information extraction method is that that convert the cipher text into the plain text by employing a secret key. Mapping the pixels into a picture is understood as extraction technique. It wants for knowledge extraction as watermarked image and therefore the secret key. For extraction method applies the inverse support vector dimension on watermarked image. With the utilization of a secret key the cryptography is finished solely. Extract the initial and therefore the watermark image. The standard of the image doesn't degrade whereas decompression. The human eyes can't sight simply. It provides the high security to the key image that cannot alter by hackers or attackers of the personal information of sender.

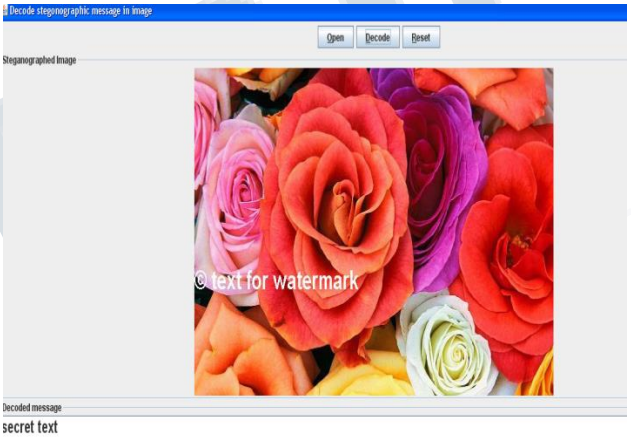


Image Decompression

The action of reversing compression is press the image to urge associate degree uncompressed image with none loss in image quality and size. Here we tend to uses DCT rule to decompress the image. Finally, the concatenated image is decompressed at the destination for viewing and analysis. The concatenated image illustration is conferred on the decoder, a reconstructed output is generated on output.

PROPOSED SYSTEM

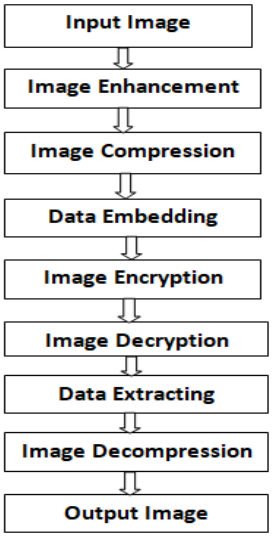
A lossless, reversible, and combined information concealment schemes is projected for public-key-encrypted pictures by exploiting the probabilistic and homomorphic properties of cryptosystems. In the lossless theme, thanks to the probabilistic property, though information of encrypted image area unit changed for data embedding, an instantaneous cryptography will still end in the initial plaintext image whereas the embedded information is extracted within the encrypted domain.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Within the reversible theme, a bar graph shrink is accomplished before coding so the modification on encrypted image for information embedding doesn't cause any component oversaturation in plaintext domain. Data embedding on encrypted domain might end in a small distortion in plaintext domain thanks to the homomorphic property, the embedded information is extracted and also the original content is recovered from the directly decrypted image. Data embedding operations of the lossless and also the reversible schemes is at the same time performed in associate degree encrypted image

Block Diagram



Performance Evaluation: Comparative execution times (in ms) of encryption algorithms with different packet size.

Input size in (Kbytes)	AES	3DES	DES
49	56	54	29
59	38	48	33
100	90	81	49
247	112	111	47
321	164	167	82
694	210	226	144
899	258	299	240
963	208	283	250
5345.28	1237	1466	1296
7310.336	1366	1786	1695
Average Time	374	452	389
Throughput (Megabytes/sec)	4.174	3.45	4.01

Comparative execution times(in ms) of decryption algorithms with different packet size

Input size in (Kbytes)	AES	3DES	DES
49	63	53	50
59	58	51	42
100	60	57	57
247	76	77	72
321	149	87	74
694	142	147	120
899	171	171	152
963	164	177	157
5345.28	655	835	783
7310.336	882	1101	953
Average Time	242	275.6	246
Throughput (Megabytes/sec)	6.452	5.665	6.347

Comparison Between Related Works

Methods	PSNR(db)	Distortion
Reversible data hiding in encrypted images	37.9	Low
Reversible data embedding using difference expansion	44	High[data large]
Expansion embedding techniques for reversible watermarking	50	Low[data small]
Lossless generalized LSB data embedding	51.1	very low

CONCLUSION

Data hiding in encrypted image is a used because of the privacy preserving requirements from cloud data management. Other methods implement RDH in encrypted images by vacating room after encryption. In these data hider can benefit it from the extra space emptied out in previous stage to make data hiding process effort-less.

REFERENCES

1) Zhenxing Qian, Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image with Distributed Source Encoding", DOI:10.1109/TCSVT.2015.2418611, IEEE, pages: 1-13.

2) Ronak Bhatia,PawanJagtap, Ashish Gupta, Professor DeeptiLawand, "Separable Reversible Data Hiding In Encrypted Image", Vol-2, Issue-6, 2016 ISSN: 2454-1362, pages: 90-92.

3) WeimingZhang n, KedeMa,NenghaiYu, "Reversibility improved data hiding in encrypted images" , Elsevier B.V., DOI:10.1016,2013.06.023 ,pages: 118-127.

4) Jiantao Zhou, Weiwei Sun, Li Dong , Xianming Liu, , Oscar C. Au, Yuan Yan Tang ,"Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation",1051-8215(c)2015 IEEE, DOI: 10.1109, pages: 1-13.

5) Xinpeng Zhang, Chuan Qin, Guangling Sun, "Reversible Data Hiding in Encrypted Images Using Pseudorandom Sequence Modulation" , IWDW 2013, pages:358–367.

6) Nilesh Solanki1, Mahesh Parmar, Dr. Vineet Richhariya, "Non-seperable reversible data hiding in encrypted image using chaoustic map, Vol. 6 (2) , 2015, ISSN: 0975-9646, pages: 1656- 1659

7) Lingling An, XinboGao, YuanYuan, DachengTao, "Robust lossless data hiding using clustering and statistical quantity histogram", 2011, Elsevier, DOI:10.1016, pages: 1-11.

8) Majid Khorramdin, Milad Amini, Nasser Torabi, Mojtaba Mahdavi, "Improving Reversible Image Watermarking using Additive Interpolation Technique", DOI: 10.1109/ISTEL.2014.7000841,pages 19-23.

9) Zhaoxia Yin, Bin Luo, Wien Hong,"Separable and Error-Free Reversible Data Hiding in Encrypted Image with High Payload", DOI: 10.1155/2014/ 604876 ,pages:1-8.

10) Jewel Vincent Chittilappilly , Tressa Micheal, "Reversible Data Hiding in Encrypted Images using Rhombus Method by RRBE", e-ISSN: 2278-2834, ISSN: 2278-8735,Volume 10, Issue 5, Ver.II (2015), DOI: 10.9790/2834-10520107,pages: 1-7.

11) Nikhila Nyapathy, Neha Tiwari, Mr. Balika J. Chelliah, "Reversible Data Hiding In Encrypted Images Using AES Data Encryption Technique", ISSN: 2278-9359 (Volume-3 Issue-4), pages:28- 35.

12) Ms. Amrutha O.C, Ms. Rabina P, "Secure Reversible Data Hiding Image Transformation Data Hiding Image Transformation Using Cloud Storage" , ISSN 0973-1873 Volume 12, Number 2(2016), pages: 193-196.

13) Dr. Sudhir S Kanade1, Durga S. Patil, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", Vol-2 Issue-1 2016,pages: 184- 192.

14) Dr.V.Khanaa, Dr.Krishna Mohanta, "Secure And The Authenticated Reversible Data Hiding In Encrypted Images", ISSN:2319-7242 Volume 2 Issue 3 March 2013, Pages : 558-568.

15) Mr. Y. Sridhar, Mr. Bighneswar Panda, GITAS, Piridi, Bobbli, "Scalable Coding of PRNG Encrypted Images", ISSN 2321-6905, Vol 1, October 2013, pages: 95-102.