Data Hiding In Encrypted Images Secured Image Watermarking System For Image Ownership

[1]A. ABINAYA, M. MANISHA, A. PRIYANGA, M. PRASANNA

[2]R. GUNASEKARAN

[1] *U.G Scholars, Dept. of Computer Science*

[2] *Assistant Professor Dept. of Computer Science*

MRK Institute of Technology Kattumannarkoil.

ABSTRACT *- In this work, we use watermarking for provide high security to images. In the era of digital information, there are multiple danger zones like copyright and integrity violations, of digital object. In case of any dispute during rights violation content creator can prove ownership by recovering the watermark. After watermarking, we use compression to reduce the size of image. And then the water marked image are splitted and shuffled in swapping method. After that we put new image over a shuffled image this method is called as masking or morphology and then encryption is performed. This is done at sender side. At the receiver side, decrypt the encrypted image with help of decryption algorithm to obtain masking image. By using the reconstruction method, we get the watermarking image. In which we split the image and text by using digital signature algorithm. For which we use several algorithms like watermarking algorithm, compression algorithm, encryption algorithm.*

I. INTRODUCTION

Cloud computing services become important solutions for the storage and continuous availability of data supplied by multiple sources. Due to the outsourcing of data and services, they are exposed to many threats that strongly increase security

Requirements in terms of [1]: confidentiality, availability and reliability (i.e. integrity and authentication). Among available security mechanisms, encryption is commonly used so as to ensure medical data confidentiality. However, once decrypted, one piece of information is no longer protected and it becomes hard to verify its integrity and its origin. From this point of view, encryption appears as an "*a priori*" protection. Watermarking has been proposed as a complementary mechanism that can improve security of medical images. When it is applied to images, watermarking modifies or modulates the image pixels' gray level values in an imperceptible way, in order to encode or insert some security attributes (i.e. the watermark) into it. As defined, such a protected image can be accessed while remaining protected by these hidden security attributes that can be used of or example for verifying the image reliability (i.e., its integrity, its origins and its attachment to one patient). Thus, combining watermarking with encryption may allow us ensuring an *a priori*/ *a posteriori* protection at the same time. In practice, watermarking is usually conducted before encryption or during the encryption/decryption processes. However, in order to watermark outsourced data without endangering privacy and data confidentiality, different approaches have been proposed so as to embed a message directly into the encrypted image, essentially in the framework of copyright protection. Three categories of approaches can be distinguished according to the availability of the embedded message into the spatial domain (i.e. after decryption process) and/or in the encrypted domain:

- *Message available in the spatial domain* (*MSD*)- The scheme proposed in [2] exploits homomorphic encryption, which allows modifying an encrypted image for the embedding of a watermark.
- *Message available in the encrypted domain* (*MED*)- As example, in [3], the image is firstly divided into patches. Before encryption, some patches are replaced by patches computed from their sparse coefficients while the residual errors in-between patches are reversibly embedded into the rest of patches; leaving thus some free space by next is used for message embedding in the encrypted domain
- *Message available in both encrypted and spatial domains* (*MSED*)- most of these methods are based on partial encryption [4] or invariant encryption [5]. With those methods, only some parts of the host image are encrypted while the rest of it is watermarked. Recently, a novel concept, called VRBE (Vacating Room Before Encryption) has been proposed in [6]. Its principle is to reversibly watermark an image before encrypting it so as to leave some free space into the encrypted domain for message embedding. However, to make possible the retrieval of this free space into the encrypted domain, the image has to be reorganized before encryption. Moreover, the decryption process is modified

so as to make possible message extraction in the spatial domain. As example, in [6] watermarkable positions in the encrypted image are placed at the beginning of the bit stream and, at the reception, watermarked positions are not decrypted.

II. EXISTING SYSTEM

In this work, a new scheme of data hiding of encrypted images for the purpose of verifying the reliability of an image into both encrypted and spatial domains has been used. This scheme couples the Quantization Index Modulation (QIM) and the Paillier cryptosystem. In this scheme, encryption/decryption processes are completely independent from message embedding/extraction. Watermarking has been proposed as a complementary mechanism that can improve security of medical images. Recently, a novel concept, called VRBE (Vacating Room Before Encryption) has been proposed. Its principle is to reversibly watermark an image before encrypting it so as to leave some free space into the encrypted domain for message embedding. The architecture of the system is relies on two main procedures: protection and verification. This can be used for verifying the image reliability even though it is encrypted.

2.1. DISADVANTAGE OF EXISTING

based on the discrete wavelet transform (DWT) and singular value decomposition (SVD).

To avoid the extraction of embedded message and protecting image reliability in both encrypted and spatial domains.

In this we use a compression algorithm, encryption algorithm, decryption algorithm, digital signature algorithm.
more robust blind watermarks.

In this work, we propose a blind watermarking scheme

2.1. ADVANTAGE OF PROPOSED SYSTEM

Computational cost is low.

Embedding the digital content into image provides high secured authentication**.**

V. SYSTEM ARCHITECTURE

The process of the design implemented with the system architecture view comprises of the parts of the project work that encapsulates all modules to be processed

III. SYSTEM

The main disadvantage of the previous work is extraction of embedded message.

During the extraction step, the knowledge of the interval (or the codebook) to which belongs to a possible attacked version of water marked image is enough to identify the embedded message.

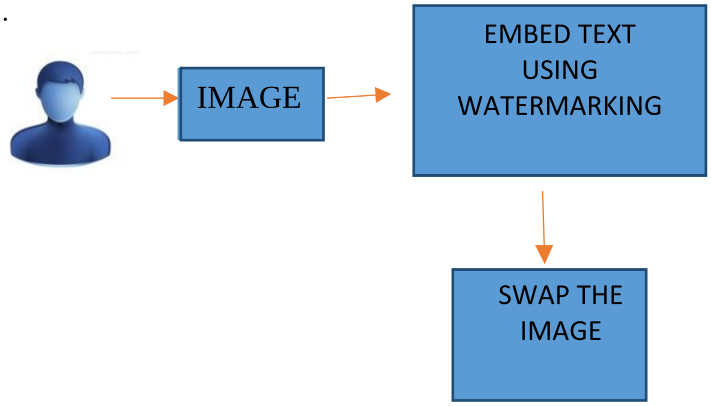
High computational cost and authentication is low.

IV. PROPOSED SYSTEM

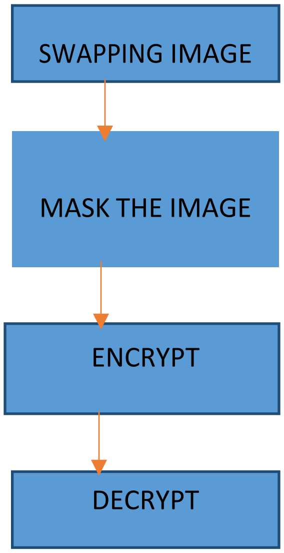
In this project, we overcome the demerits of previous work.

In recent years it has been recognized that embedding information in wavelet transformation domain leads to

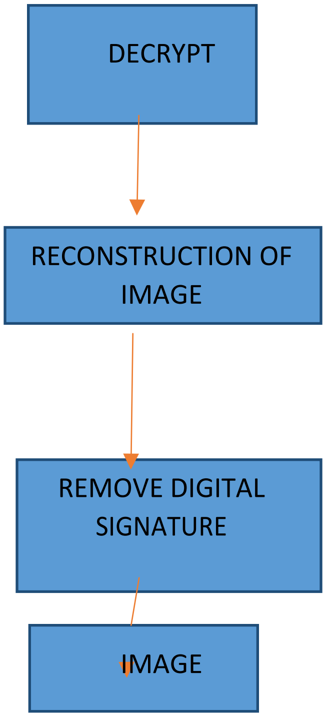
.



MODULES DESCRIPTION

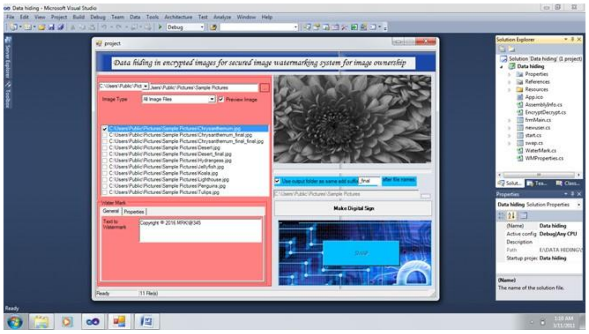


AFTER DECRYPTION:



4.1. IMAGE AS INPUT

We give image as input, process an image in 2x2 pixel blocks. This allows flexibility in tracking the edges and also achieves high computational complexity. The two processing cases that Flipping the candidates of one does not affect the *flippability* conditions of another are employed for *orthogonal embedding*.


Data hiding - Microsoft Visual Studio

project

Data hiding in encrypted images for secured image watermarking system for image ownership

Image Type: All Image Files ☑ Preview Image

☑ C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum_final.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum_final_final.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Desert.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Desert_final.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Koala.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg
□ C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg

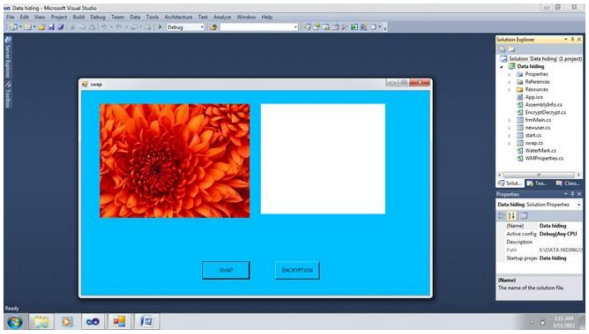
Text to Watermark: Copyright © 2016 MRK!@345

☑ Use output folder as same add suffix _final after file names

Ready 11 File(s)

4.2. TEXT EMBEDDING

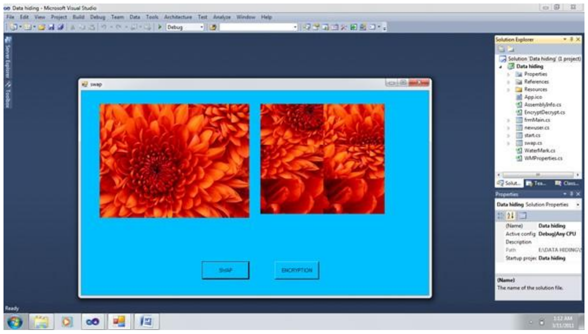
Watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark. Watermarked content can prove its origin, thereby protecting the data.


Data hiding - Microsoft Visual Studio

swap

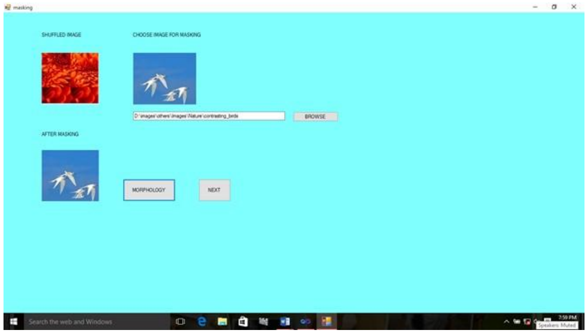
4.3. SWAPPING THE IMAGE

We flip an edge pixel in binary images is equivalent to shifting the edge location horizontally one pixel and vertically one pixel. A horizontal edge exists if there is a transition between two neighboring pixels vertically and a vertical edge exists if there is a transition between two neighboring pixels horizontally.



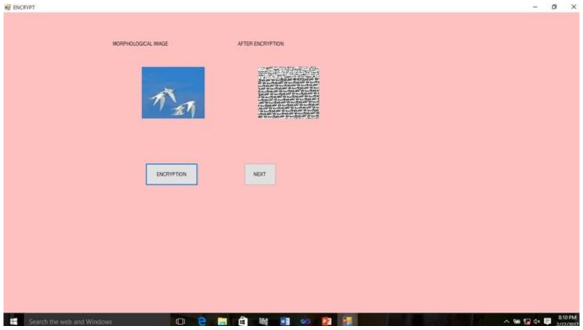
4.4. MASK THE IMAGE

After swapping the image we have to mask the swapping image by using a new image. This process is called as morphology. In this we put a new image over the already shuffled image. By using this method we can confuse the hackers and avoid them from extracting the content.



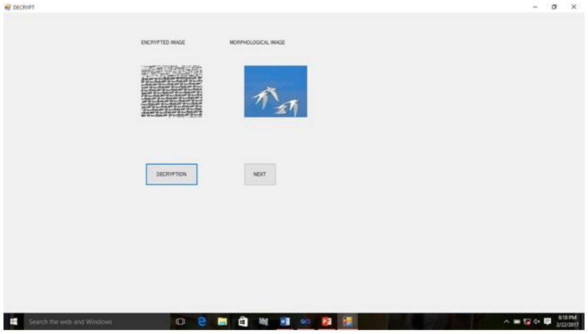
4.5. ENCRYPTION

In this module we encrypt the data embedded image. The purpose of authenticator watermark of a block is invariant in the watermark embedding process, hence the watermark can be extracted without referring to the original image. The encryption techniques used in this module.



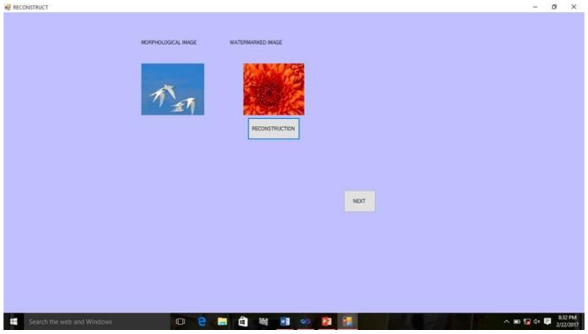
4.6. DECRYPTION

In this module we decrypt the encrypted image. The purpose of decryption of encrypted image is to obtained the morphological image, hence this is the process of recovering the original image to obtained the image and text. Watermark can be extracted after this module. The decryption techniques used in this module.



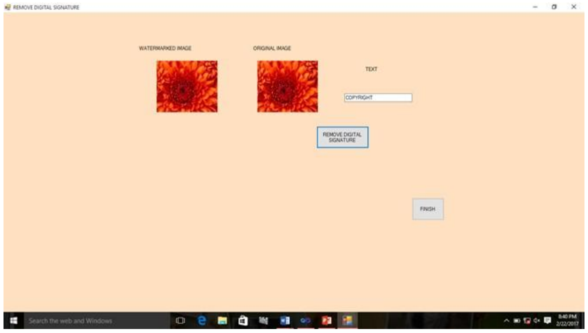
4.7. IMAGE RECONSTRUCTION

We have to reconstruct the image after the decryption to obtain the watermarked image. In this method we directly recover the image which has embedded with text. We handle the swapping image also in this module. In this method the masked image is removed and then shuffled image is rearranged.



4.8. REMOVE DIGITAL SIGNATURE

After reconstructing the image, the main process is to remove the text from the image. This process is often called as removing digital signature. This is the final process in which we get the image and text separately. As user wish either a text or an image be the password.



TEXT

COPYRIGHT

VI. EXPERIMENTAL RESULTS AND DISCUSSION

Experiments were conducted on 100 8-bit depth ultrasound images of 576×688 pixels. Two indicators are considered to evaluate the performance of our system: capacity and watermark imperceptibility.

Capacity: Because one bit of message is embedded per pixel subset, the capacity one can insert into an image depends on the dimensions of the pixel subsets and of the image. Indeed, the achieved capacity rate is equal to $1/p$ bpp (bit per pixel). Working with p=1 leads to a capacity of 1bpp or equivalently to a message of about 396 *K*bits. This capacity is large enough for the insertion of some security attributes assessing the image reliability. For instance, M may contain an authenticity code (e.g. about 1000 bits by combining the French National Identifier with the Unique Identifier of DICOM the standard for medical images [9]), and an integrity proof which can be a secret pseudorandom binary sequence [10]. The integrity of the encrypted or decrypted image can thus be checked based on verifying the presence of this sequence within the image. Moreover, one can better enhance the robustness of the embedded message in the encrypted domain by working with p>2; allowing repeating the message at least 3 times.

Distortion: As our algorithm introduces in average the same image distortion in each pixel block, we decided to use the Peak Signal to Noise Ratio (PSNR) to measure the distortion between the image I and its watermarked and deciphered version I_w. The lower bound of PSNR can be theoretically determined according to □. Let us assume that the pixels of the image (i.e. I) are uniformly distributed over the cells of QIM codebooks .This means that the probability that one subset pixel I_i^j belongs to the cell that encodes ‘0’ (resp. ‘1’) is 0.5. Since W is a binary sequence uniformly distributed, the probability that the pixel I_i^j belongs to the cell that encodes w_i is 0.5.

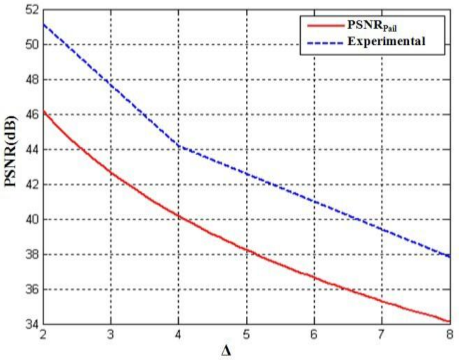


FIG.1: Lower theoretical PSNR bound (*PSNR_{Pail}*) and obtained experimental PSNR values for different values of Δ.

VII. CONCLUSION

In this work, we have proposed a new data hiding scheme of encrypted images that allows accessing a message in both the encrypted and spatial domains. This message can be used for verifying the image reliability even though it is encrypted. Its originality stands on the use of a prewatermark which makes the insertion /extraction processes independent of the encryption/decryption processes, and vice versa. We have also provided an implementation of our scheme based on QIM modulation and Paillier cryptosystem. It provides an important capacity rate while minimizing image distortion. Future works will focus on making this implementation more robust to attacks like lossy image compression and on enhancing the quality of the watermarked images.

And we just introduce this concept of passing the secured password over the image. Future work will focus on making the password send by the user and the encrypted embedded image is reconstructed and remove the text from the image by the receiver.

REFERENCES

[1]. D. Bouslimi, *et al.*, “A telemedicine protocol based on watermarking evidence for identification of liabilities in case of litigation”, *Health com* (2012), 506-509.

[2]. N. Memon, P. Wong, “A buyer-seller watermarking protocol”, *IEEE Transactions on Image Processing,* (2001) 643–649.

[3]. X. Cao, *et al.*, “High capacity reversible data hiding in encrypted images by patch-level sparse representation”, *IEEE Transactions on Cybernetics*, 2015.

[4]. D. Xiao, S. Chen, “Separable data hiding in

encrypted image based on compressive sensing", *Electronics Letters*, 50 (8) (2014) 598–600.

[5]. R. Schmitz, *et al.*, "Towards more robust commutative watermarking encryption of images", *IEEE International Symposium on Multimedia (ISM)* (2013) 283–286.

[6]. K. Ma, *et al*, "Reversible data hiding in encrypted images by reserving room before encryption", *IEEE Transactions on Information Forensics and Security*, 8 (3) (2013) 553–562.

[7]. B. Chen, G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital watermarking and information embedding," *IEEE Trans. on Information Theory*, 47(4) (2001), 1423- 1443.

[8]. P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity classes", *Proc Eurocrypt*, 1592 (1999) 223-238.

[9]. W. Pan, *et al., "*Medical image integrity control combining digital signature and lossless watermarking", In *Data privacy management and autonomous spontaneous security*. Springer Berlin Heidelberg, (2010), 153-162.

[10]. D. Bouslimi, *et al.*, "A joint encryption/watermarking system for verifying the reliability of medical images", *IEEE Transactions on Information Technology in Biomedicine* 16 (2012) 891–899.

[11]. K. Chen, T.V. Ramabadran, "Near-lossless compression of medical images through entropy coded DPCM", *IEEE Transactions on Medical Imaging*, 1994.