International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Dual Image Watermarking using Symmetrical IB Algorithm

J. Priscilla Sasi, P. Arul

Abstract: ***The technique of watermarking is used to safeguard the copyright protection and used to prove the proprietorship of certain images, documents, audio and video files. This paper presents a new scheme where the final digital image is created after embedding one watermark inside another watermark (dual watermark), scrambled the image to safeguard from intruders and then embedded into the main digital image. The dual watermark mechanism improves the capacity of the data to be watermarked and more importantly the dual watermarked image is encrypted using symmetrical encryption algorithm (IB algorithm) an improved version of the blowfish algorithm to increase the security and makes it harder for the intruders to crack the watermark.***

Keywords: security, watermarking, symmetric encryption, digital image, LSB

I. INTRODUCTION

The increasing usage of the internet among the current generation has caused an alarming issue with respect to ownership rights of the audio, video and image files and this it is imperative to provide an excellent solution to curtail the data privacy which is considered as a major concern. Many new techniques with various needs related to watermarking have emerged recently but still there is a huge requirement regarding a tamper free technique to evade the copyright and privacy related problems. Digital watermarking was first used in the thirteenth century by some Italians in their arts to conceal some important secrets invisible to the naked eyes. Digital watermarking is a process of concealing data in the form of watermark in the digital files and later can be extracted to prove the ownership of the digital file when litigation arises or the file is altered without the consent of the owner. In simple words the watermark is the data hiding or carrying media in a digital file to prove the proprietorship. The data present in the watermark can be copyright details of the file, owner's name, firm name or details related to the license which can be visible as well as invisible to the people.

The term "watermark: was actually originated from the German word "wassermarkke" and this name is provided to it because it contains water like effect of the image.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Mrs. J. Priscilla Sasi*, pursuing her Ph.D degree in Government Arts College, Thuvakudi, Tiruchirappalli,
Dr. P. Arul, Assistant Professor in the Department of Computer Science, Government Arts College, Thuvakudi, Trichy.

The water mark was invented long back by the Chinese during the usage of paper and in the eighteenth century the watermark is used to denote the manufactured date but nowadays the watermarking is used to evade the counterfeiting and to avoid the frauds involved in ownership and copyrights. Many countries use the watermark in their currencies to curtail the forgery and today the paper watermarking has completely replaced by the digital watermarking

II. RELATED WORKS

The authors Yusuk Lim, Changsheng Xu and David Dagan Feng created a web based authentication system to provide watermarking on their images for their registered users in the year 2001 [1]

The author Nameer N. EL-Emam in the year 2007 [2] proposed least significant bit method combined with steganography to enhance the security and developed a secure model impossible to break.

The author Zhu et al. in the year 1999 presented a multi-resolution watermarking technique which embeds in all the high pass bands in a nested manner at numerous resolutions. But in this method the HVS aspect is not considered and later the authors Kaewkamnerd and Rao [3] improved this method by adding the HVS factor during watermarking.

The authors Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang proposed a method in the year 2005 where the Watermark is hidden in watermark using vector quantization and this watermark nesting increased the embedding capacity for watermark [4].

The authors G. Sahoo and R. K. Tiwari in the year 2008 [5] proposed a method that works on several images using file hybridization technique and implemented the cryptography to embed two information files using the concept of Steganography.

The author Preeti Gupta in the year 2012 [6] proposed cryptography based digital nested watermarking where the embedding and extraction is carried out using simple cryptology. The encryption and decryption of watermarks was carried out using XOR operation.

Author (s) can send paper in the given email address of the journal. There are two email address. It is compulsory to send paper in both email address.

III. PROPOSED APPORACH

Plethora of watermarking methods is developed and the most important and vital method used in most of the data security is the least significant bit LSB method. This method is the easiest one which embeds the precious data in the least significant bit of the main object.

The main advantage of this method is that if the watermark size is small it can be added multiple number of times and during the extraction at least one watermark will be survived and retrieved. The LSB method is illustrated in the following figure 1 where the input image is considered and the watermark image is taken and the bits are added to the LSB of the input image as shown in the figure to get the output image.

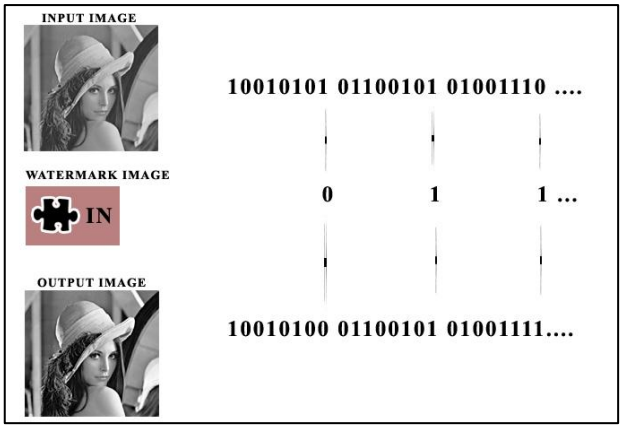


Fig. 1. LSB method to embed the watermark data.

Simply embedding the watermark data will not be ideal and the intruders will find it easier to crack and gain access to the data to modify or misuse the hidden precious data and to make the LSB method effective and secure enough to be tamper proof, cryptology is applied before embedding. The proposed approach utilizes two water marks (dual watermark) to enhance the security and more importantly the dual watermarked image is scrambled to distort the image to protect it from the offenders and finally cryptography (i.e.) symmetric encryption scheme is employed as shown in the following work flow diagram.

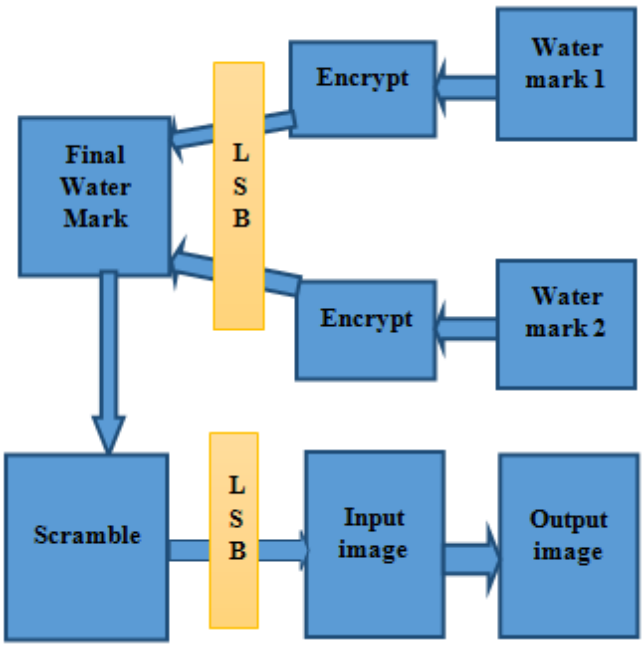


Fig. 2. The workflow of the proposed scheme.

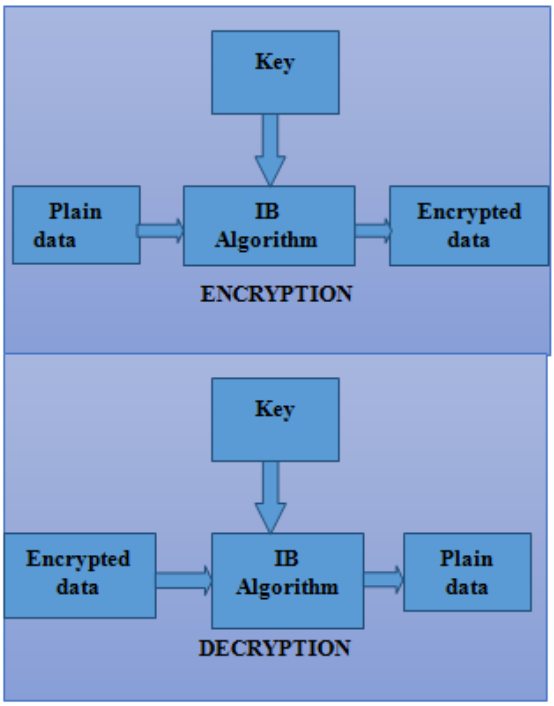
The symmetric encryption scheme employs the same key for encryption as well as decryption and it is the simplest cryptography method available for implementation. The symmetric algorithm employs block cipher which is nothing but dividing the data into small blocks of fixed length during the encryption and decryption processes. The proposed IB algorithm is an improved version of the blowfish algorithm developed by Bruce Schneier [7] in the year 1993. The key used in the proposed algorithm is big in size and varies between 32 and 1120 bits. The proposed algorithm utilizes divides the key into fixed size sub arrays comprising of 18 parts and then iterates 16 times as in the blowfish algorithm to carry out the encryption process. The IB – Improved Blowfish algorithm's encryption process is shown in the figure 3.

```
Procedure IBEncryption(Input data D, KeyParts K)

INPUT: Input plain data D, Key parts K(18 parts)
OUTPUT: Final Cryptic Text
BEGIN:
    Load the Input plain data D→64 bit
    Divide D / 2 and store in DLEFT and DRIGHT
    ∀ I = 1 to 16 do begin
    DLEFT = DLEFT XOR KI
    DRIGHT = DLEFT XOR DRIGHT
    Interchange the values in DRIGHT and DLEFT
    END FOR
    Interchange the values in DRIGHT and DLEFT
    DRIGHT = DRIGHT XOR K17
    DLEFT = DLEFT XOR K18
    FinalCrypt = DLEFT APPEND DRIGHT
    Return FinalCrypt
END PROCEDURE
```

Fig. 4. Pseudo code of the improved blowfish algorithm encryption.

The proposed improved blowfish algorithm enhances the overall security of the data that are being encrypted and speeds up the entire process without any lag in time and improves the goodness index considerably. The goodness index is the percentage of change that has happened to the plain text and the value of the GI lies between 0 and 1 with 1 being the highest value where the plain text is entirely converted into some unknown cipher text. The decryption process is the inverse of the encryption process shown in the figure 4 and the same 18 keys are being used for this process but in reverse order. The encryption and the decryption process present in the proposed IB algorithm is shown in the figure 5.



The main advantage of the proposed approach is encrypting the secret data to be watermarked initially and then embedding the encrypted secret data into another dummy encrypted image before embedding the blended encrypted water marked image into the main image which obviously increase the security aspect and then of course increase the overall capacity of the watermark data into the main image.

The LSB insertion of bits is nothing but replacing the last bit in a byte by the insertion data bits which is shown in the following figure 6 which is actually quicker and easier to embed bits in the binary data without any complexity related to calculations. The pseudo code of the procedure is showcased in the following figure.

```
Procedure LSBinsertion(data D, InsertionData Id)

INPUT: data D, InsertionData Id
OUTPUT: Output mixed data
BEGIN:
    Load the Input data D
    Load the Insertion data bits Id
    Flag=0
    RESULT = ϕ
    ∀ Byte B ∈ D do begin
    Fetch B
    Replace the last bit in B by Insertion data bit Id[Flag] →R
    RESULT = RESULT + R
    Increment the Flag by 1
    END For
    Return RESULT
END PROCEDURE
```

Fig. 6. Pseudo code of LSB insertion of data.

The worked example of the insertion or replacement of the least significant bit is shown in the figure 1 where the last bit in a byte is replaced by the water marked data bits and this will definitely increase the security level up to a greater altitude. The scrambling or jumbling the image is carried out by the procedure shown in the figure 7.

IV. SCRAMBLE IMAGE

The dual watermarked image is scrambled and jumbled to ensure that the original watermarked image is not visible to the attackers and guarantees a high goodness index in this method.

```
Procedure ScrambleData(Input data D)

INPUT: Input data D
OUTPUT: Scrambled data
BEGIN:
    Load the input data D
    Convert the data to binary→Bdata
    Bifurcate Bdata and store it in→B1, B2
    While (B1 ≠ EOF)
     Fetch Byte from B1 and B2
     Append them →RES
     END While
    Reverse RES →RES1
    Interchange the alternate bits in RES1→RESULT
    Return RESULT

END PROCEDURE
```

Fig. 7. Pseudo code to scramble the data.

V. DIW ALGORITHM

The proposed dual image watermarking algorithm is showcased in the following figure and its overall workflow is also showcased in this section.

```
Algorithm DIW(Input data D, dataONE d1, dataTWO d2)

INPUT: Input data D, dataONE d1, dataTWO d2
OUTPUT: Watermarked data
BEGIN:
    Load dataONE d1, dataTwo d2, data D
    W1= IBEncryption(d1, Key1)
    W2 = IBEncryption(d2, Key2)
    WF= LSBinsertion(W1, W2)
    SD = ScrambleData(WF)
    Output= LSBinsertion(D,SD)
    Return Output
END PROCEDURE
```

Fig. 8. Pseudo code of the Dual Image Watermarking DIW algorithm.

The block diagrams of the embedding or the encoding process are shown in the following figures 9 and the decoding process is the reverse of this process.

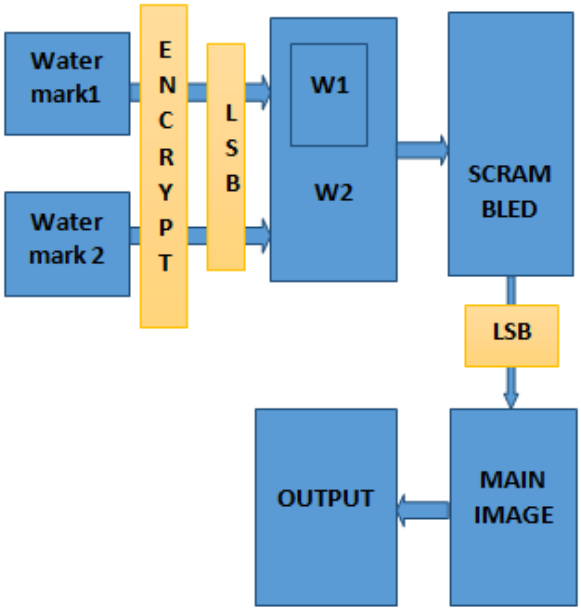


Fig. 9. Encryption process of DIW algorithm.

VI. EXPERIMENTAL EVALUATION

In the experiments the images of 450 X 300 sized is used and the entire procedures in the algorithm is implemented using C#.NET and a detailed evaluation is carried out regarding the correlation coefficient values of the retrieved watermarks by various attacks. The evaluated results are showcased in the following section.

The proposed algorithm's performance is judged after applying various attacks on the watermarked images and then compared with other existing approaches to justify the overall security level of the method proposed in this paper. The approaches compared here is DWT blended with SVD [8] and the SVD based Chaos encryption algorithm [9]. Initially the proposed method's process with an example image is showcased in the figure 10.

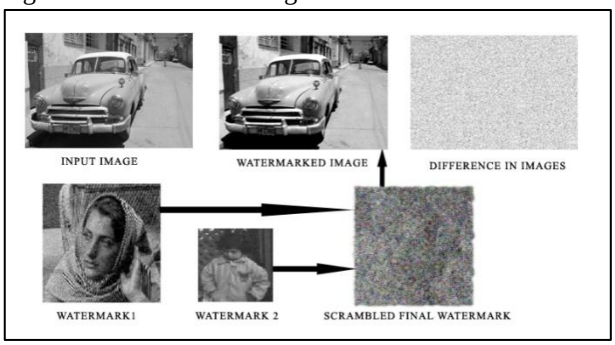


Fig 10: Overall Process of the DIW algorithm.

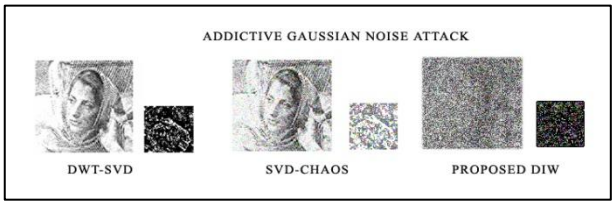


Fig. 11. Additive Gaussian attack and retrieved watermarks.

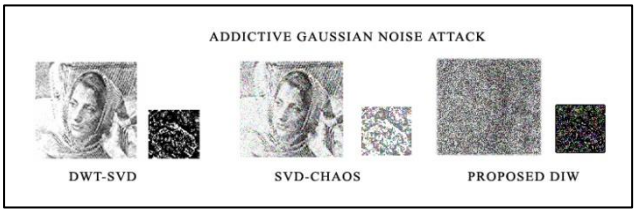


Fig. 12. Median Filter attack and retrieved watermarks.

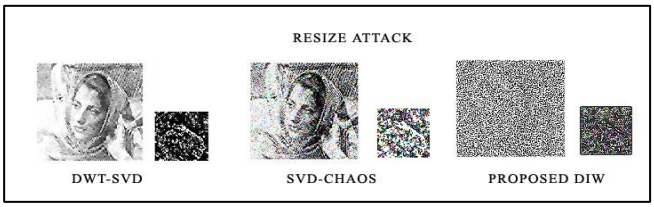


Fig. 13. Resize attack and retrieved watermarks.

From the figures 11, figure 12 and figure 13 the retrieved watermarks are shown and the correlation coefficients of the extracted watermarks are manipulated as shown in the comparison table I.

Table - I: Correlation coefficient of the retrieved watermarks W1 and W2.

APPROACH	GAUSSIAN		MEDIAN		RESIZE	
	W1	W2	W1	W2	W1	W2
DWT-SVD	0.897	0.452	0.883	0.421	0.893	0.433
SVD-CHAOS	0.899	0.412	0.873	0.416	0.876	0.418
PROPOSED	0.102	0.023	0.092	0.016	0.101	0.067

VII. CONCLUSION

In the experiments the images of 450 X 300 sized is used and the entire procedures in the algorithm is implemented using C#.NET and a detailed evaluation is carried out regarding the correlation coefficient values of the retrieved watermarks by various attacks. The evaluated results are showcased in the following section.

REFERENCES

1. Yusuk Lim, Changsheng Xu and David Dagan Feng, "Web based Image Authentication Using Invisible Fragile Watermark", 2001, Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia, Page(s): 31 – 34.
2. Nameer N. EL-Emam "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science. April 2007, Page(s): 223 – 232.
3. Kaewkamnerd, N., Rao, K.R., "Wavelet based image adaptive watermarking scheme" in IEE Electronics Letters, vol.36, pp.3 12-313, 17 Feb.2000.
4. Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan, "Hiding Watermark in Watermark", in IEEE International Symposium in Circuits and Systems (ISCAS), Vol. 4, pp. 4018 – 4021, May 2005
5. G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganography"
6. Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012.

7. B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), "Fast Software Encryption", Cambridge Security Workshop Proceedings, (December 1993), Springer-Verlag, 1994, pp. 191-204.
8. Gaurav Bhatnagar, Balasubramanian Raman and K. Swaminathan, " DWT-SVD based Dual Watermarking Scheme", HIEEE International Conference on the Applications of Digital Information and Web Technologies (ICADIWT2008) H, pp. 526-531.
9. R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, 2002, pp. 121-128.

AUTHORS PROFILE

Mrs. J. Priscilla Sasi, ccompleted her B.Sc., (Physics) and M.Sc (Computer Science) degree respectively from Indira Gandhi Arts & Science College and Bishop Heber College, Bharathidasan University, Tiruchirappalli, Tamil Nadu in April 2000 and April 2003. She completed her M.Phil degree in Bharathidasan University, Tiruchirappalli during March 2008. After M.Phil studies she worked as Assistant Professor in Bishop Heber College, Tiruchirappalli for 2 years and worked as Assistant Professor in Guru Nanak College, Chennai for 8 years. Currently she is pursuing her Ph.D degree in Government Arts College, Thuvakudi, Tiruchirappalli, affiliated to Bharathidasan University for research work in Network Security. Her research mainly focused on to prevent Data theft which is based on human factor information security.

Dr. P. Arul obtained his B.Sc., (Computer Science) and MCA., degree from Hans Rover Arts College, Perambalur, Tamil Nadu, in 1988 and 1994 respectively. He received his M.Phil, from Bharathiyar University , Coimbatore, Tamil Nadu, in the year 2000. He received his Ph.D., from Vinayaka Mission, Salem, Tamil Nadu, in the year 2010. He has published more than 10 research papers in national and international journals. For 2 years worked as Assistant Professor in the Department of Computer Science, Cheran Arts and Science College, Erode. For a decade he worked as Assistant Professor in the Department of Computer Applications of Kongunadu Arts and Science College, Coimbatore. He also worked as Assistant Professor in the Department of Computer Science, CMS Arts and Science College, Coimbatore for 3 years. Currently he is working as Assistant Professor in the Department of Computer Science, Government Arts College, Thuvakudi, Trichy. He is supervising four doctoral works in Computer Applications. His mission is to impart qality, concept oriented education and mould younger generation.