Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm

Jasdeep Singh Bhalla[*], Preeti Nagrath[**]

[*] Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi

Abstract- Digital watermarking is referred to a method used for copyright protection and authentication. In this paper, we present a method of nested digital watermark embedding and extraction in which a nested watermark (a watermark inside another watermark) is embedded into the main image. This concept of nested watermarking is used to increase the watermark embedding capacity. In this method, a watermark is embedded into another watermark which is considered as the main watermark and then this main watermark is embedded into the cover image (main image). These watermarks are encrypted before embedding in order to have increased safety, thus to perform encryption and decryption process we used the Blowfish algorithm. Therefore, our research work is focused on increasing the embedding capacity and improving security of the watermarks.

Index Terms- Digital Watermarking, Blowfish, Image Watermarking, copyright protection, Least Significant Bit, Nested Watermark

HISTORY OF WATERMARKS

The term "watermark" was originated from the German term "wassermarke". The name 'watermark' is given because these marks have a resemblance towards the effects of water on paper [21]. The ancestors of Digital watermarks were the paper watermarks, as papers were invented in China over a thousand years ago. However, the first paper watermark was created in 13th century, in Italy [21]. In the 18th century, the watermarks had been used as trademarks to record the manufactured date, or to indicate the size of original sheets. These days, watermarks are commonly used on bills to avoid counterfeiting, documents for copyright protection. Most of the developed countries today use watermarks in their paper currencies and postage stamps to make forgery/infringement more difficult.

The digitisation of our world has expanded our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims. However, Digital Watermarks have replaced paper watermarks almost completely.

I. INTRODUCTION

With the widespread use of Internet and increasing rate of development in Information Technology industry, the digital media files (such as images, audio files, documents and videos) are easily accessible and acquired in our daily life from the internet. Due to this, original digital multimedia contents suffer from infringement of their copyrights, easy modification and fast content transfer over the Internet. As a result, data piracy and copyright protection has become a serious issue in order to protect one's ownership rights. Hence, some protection measures are needed to be employed to conquer this major problem that would only be increasing as time progresses. Sensing the need, many new techniques have been developed in recent times and the research is still ongoing for new techniques of information hiding and security. A very important technique that had come into existence for the first time in Italy, in the 13th century was *Digital watermarking*. Digital watermarking is the process of embedding data referred to as a watermark, tag or a label into a multimedia file in such a way that it can be detected or extracted by the owner to make necessary assertions about the illegal modifications of the media that were done without owner's approval. The media file can be any digital file such as image, video, audio or text. In other words, a watermark can be explained as a carrier of information (data). This Information can constitute the copyright details of the file, license, tracking and authorship details of the media etc. The watermark may or may not be visible to the user/viewer of the file.

II. EXISTING TECHNIQUES

- A method in which the multimedia content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key was developed by Miroslav Dobsicek [1].
- In 2001, a web based authentication system was developed by Yusuk Lim, Changsheng Xu and David Dagan Feng. In case of watermark embedding, it is installed in the server as an application software that any authorized user (who has the access to the server) can generate watermarked image [2].
- In 2003, a new method which manipulates "flappable" pixels to enforce specific block based relationship in order to embed a significant amount of data without causing noticeable artifacts was developed by Min Wu and Bede Liu [3].
- In 2005, Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al- Taani explained a method consisting of three steps. First, the edge of the image is detected using Sobel mask filters. Second, the least significant bit LSB of each pixel is used. Finally, a gray level connectivity is applied using a fuzzy approach and the ASCII code is used for information hiding. The given method embeds three images in one image and includes, as a special case of data embedding, information hiding, identifying and authenticating text embedded within the digital images [6].

- In 2006, Harpuneet Kaur, R. S. Salaria proposed a method of nested watermark embedding and extraction for increasing the embedding capacity of watermarks and increasing security of the watermarks by their encryption [4].
- In 2007, a method was proposed by Nameer N. EL-Emam in which data security using LSB insertion steganographic method was introduced. In this approach, high security layers have been proposed through three layers to make it difficult to break through the encryption of the data [5].
- In 2008, an approach to hide huge amount of data using LSB Steganography technique was proposed by Prof S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das. They have given much emphasis on space complexity of the data hiding technique [8].
- In 2008 , G. Sahoo and R. K. Tiwari proposed a method that works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using Steganography [10].
- In 2012, Preeti Gupta proposed a cryptography based digital watermarking method in which the embedding and extraction of nested watermarks was done. Encryption and decryption of watermarks was done using XOR operation [7].

A) WATERMARK EMBEDDING TECHNIQUES

There are various watermark embedding techniques that have evolved in recent times but we specifically used LSB technique [20] for embedding watermarks into main image.

Least Significant Bit (LSB) Technique

The most straightforward method that can be used for watermark embedding would be to embed the watermark into the least significant bits of the main object (cover object) [20]. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success. An example is given below:

Let us consider:
A= Original Image
B= Watermark
C= Watermarked Image

Embedding Procedure

A: 10000100 00100101 10001000 01010001…
B: 1 0 0 1…
C: 10000101 00100101 10001000 01010001…

It can be inferred from the above example that the watermark's (in this case, B) binary bits are added to the least significant bits of the original image (in this case, A). Least Significant Bit substitution will survive transformations such as cropping effectively, but with any addition of noise or lossy compression it will adversely affect the watermark.

B) ENCRYPTION AND DECRYPTION TECHNIQUES

Blowfish Algorithm

Blowfish is a symmetric encryption algorithm, which makes the use of the same secret key for both encryption and decryption of the message. It is a block cipher which means that it divides the message into blocks of fixed length during encryption or decryption This algorithm is used as an alternative for DES (Data Encryption Standard) or IDEA International Data Encryption Algorithm) [17]. It takes a variable-length key, ranging from 32 bits to 448 bits. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then, it has been slowly gaining acceptance as a strong encryption algorithm. Blowfish is not patented, is license-free, and is available free for all uses [12].

Blowfish Algorithm is a Feistel Network, in which a simple encryption function is repeated 16 times. The block size is 64 bits, and the key can be of any length up to 448 bits [13]. This algorithm is suitable for applications in which the key does not change very frequently. It is comparatively faster as compared to other encryption algorithms over handling of larger data. A Feistel network is a general method of transforming any function into a permutation. It was invented by Horst Feistel and has been used in many block cipher designs [13].

This algorithm consists of two parts :

- *Key-expansion part:* In Key expansion, a key of at most 448 bits is being converted into several subkey arrays totalling 4168 bytes.
- *Data- encryption part:* In Data encryption, 16-round Feistel network is used. Each round consists of a key dependent permutation, data-dependent substitution and a key. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [13].

Blowfish uses a large number of subkeys during its execution. These keys are computed before data encryption or decryption [12].

- The P-array consists of 18 subkeys (32 bit): P1, P2,..., P18.
- There are four S-boxes (32 bit) with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

Encryption

Blowfish has 16 rounds. The input is a 64-bit data element, x.

Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Then, xR = xR XOR P17 and xL = xL XOR P18.

Finally, recombine xL & xR to get the cipher text [12]. Process of encryption is shown in figure 1.

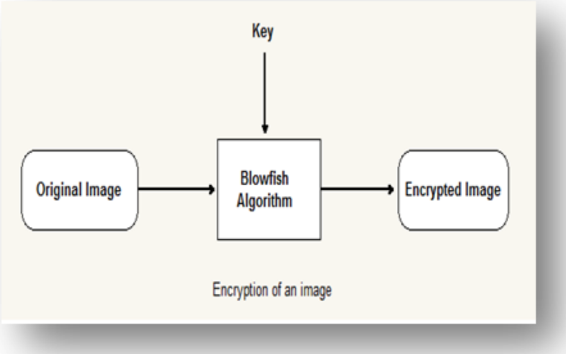

Figure 1: Encryption of image using Blowfish Algorithm

Decryption

The process of decryption using blowfish algorithm is shown in figure 2. In this process, an already encrypted image is decrypted using the same key that was used at the time of encryption. Decryption process is similar to encryption except that in decryption, P1,P2, … P18 are used in reverse order [13].

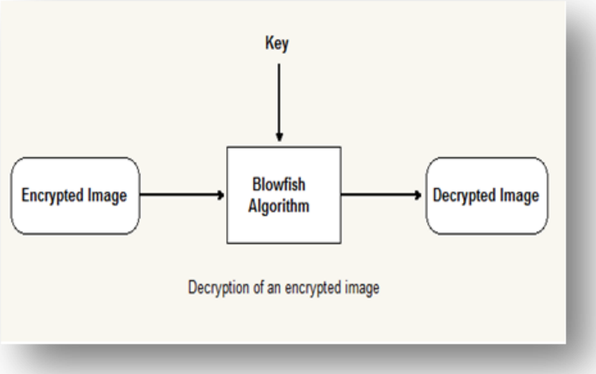

Figure 2: Decryption of image using Blowfish Algorithm

III. PROPOSED METHOD

In this paper, we are proposing a nested digital watermarking technique of watermark embedding and extraction. 'Nested' here basically means a watermark embedded into another watermark. In this method, one watermark is encrypted (using *Blowfish Algorithm*) and embedded into another watermark and this nested watermark (watermark embedded into another watermark) is again encrypted and finally embedded into the main cover image. This concept is shown in figure 3. This method provides an additional level of security for watermarks due to encryption of watermarks. It also increases the embedding capacity of a watermark (due to use of nested watermarks) as compared to the method in which a single watermark is embedded into an image for protecting copyright infringement.

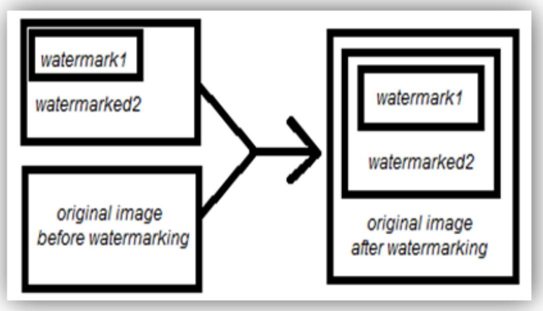
watermark1
watermarked2
original image before watermarking
watermark1
watermarked2
original image after watermarking

Figure 3: Watermark Embedding Process

For embedding first watermark in second, we used the spatial domain technique (LSB) as it is concise and less time consuming as compared to the frequency or wavelet domain techniques. *Least Significant Bit (LSB)* technique basically inserts the watermark bits to the least significant bits of the main image. By using LSB technique, first watermark is embedded into the second watermark. And then this second watermark is embedded into the main image. This technique is explained above in section II(A).

For encryption and decryption of watermarks, the *Blowfish Algorithm* is used as it is an efficient technique. The *Blowfish Algorithm* is explained above in section II(B). The first watermark is encrypted before embedding it to the second watermark. After first watermark is embedded into the second watermark, the nested watermark (one watermark inside another watermark) is encrypted again and finally embedded into the main image.

Watermark Embedding

Abbreviations that are used in this algorithm:

Watermark1: Primary watermark image.
Watermark2: Secondary watermark image (Main watermark).
Main Image: Original image that is to be watermarked.
Y1: Key for encrypting *Watermark1.*
Y2: Key for encrypting *Watermark2.*
W1: Key for embedding *watermark1.*
W2: Key for embedding *watermark2.*

Embedding Algorithm

1. *Watermark1* is encrypted by using *Blowfish Algorithm* with key *Y1*. Output is called *Encrypted1*.
2. *Encrypted1* is embedded into Watermark2 using key *W1*. Output image is *Watermarked1*.
3. *Watermarked1* is encrypted by using *Blowfish Algorithm* using key *Y2*. Output image is *Encrypted2*.
4. *Encrypted2* is embedded into *Main image* using key *W2*. Output is *Watermarked2*.

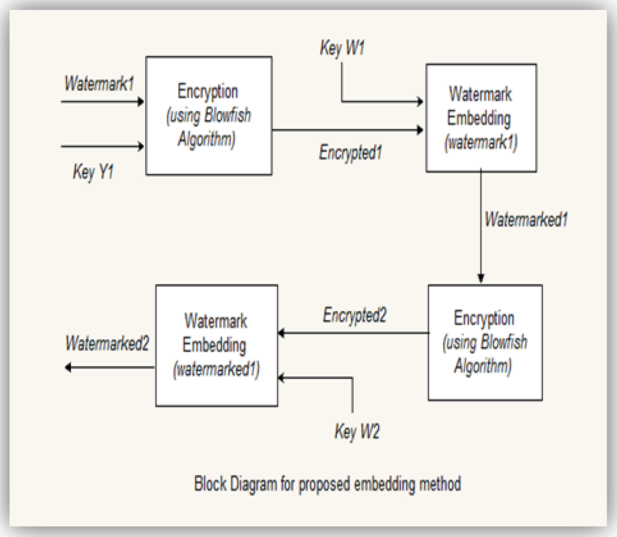
Watermark1
Key Y1
Encryption (using Blowfish Algorithm)
Key W1
Encrypted1
Watermark Embedding (watermark1)
Watermarked1
Encrypted2
Watermarked2
Watermark Embedding (watermarked1)
Encryption (using Blowfish Algorithm)
Key W2
Block Diagram for proposed embedding method

Figure 4: Block Diagram for embedding method

Output

Watermarked Image: *Watermarked2*.

Watermark Extraction

Inputs

Watermarked2': Already watermarked image.
S1: Size of watermark1.
S2: Size of watermark2.
Y2: Key for decrypting recovered watermark from cover Image.
Y1: Key for decrypting recovered watermark from main watermark (secondary watermark).
W2: Key used for recovering encrypted watermarked watermark from Main Image (cover image).
W1: Key for recovering encrypted watermark from the main watermark.

Extraction Algorithm

1) Extract encrypted *Watermark2* from *Watermarked2* using key *W2*. Output is *Encrypted2'* (recovered image).
2) Decrypt *Encrypted2'* using *Blowfish Algorithm* with key *Y2*. Output is *Recovered2*.
3) Extract encrypted *Watermark1* from *Recovered2* using key *W1*. Recovered image is called *Encrypted1'*.
4) Decrypt *Encrypted1'* using *Blowfish Algorithm* with key *Y1*. Output is *Recovered1*.

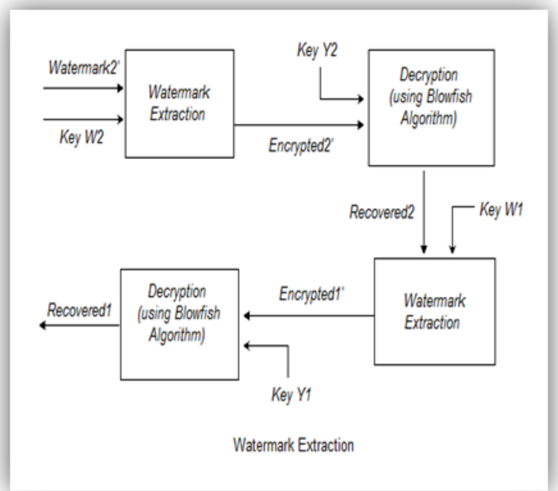

Figure 5: Block Diagram of Watermark extraction process

Output

Recovered2: Main watermark recovered from *Watermarked2* (Already watermarked image)

Recovered1: Watermark recovered from the main watermark.

IV. EXPERIMENTAL RESULTS

In our experiment, we used 450x300 sized images for executing our method of watermarking.

Simulation Tool Used: Matlab R2012b

The above proposed method was executed using Matlab R2012b software. Matlab is a registered product of Mathworks Inc, Copyright 1984-2012.

Figure 6: Watermark1

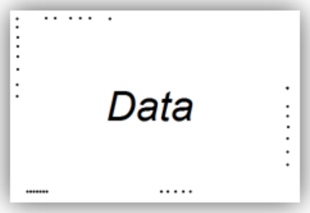

Figure 7: Watermarked watermark (watermark2)

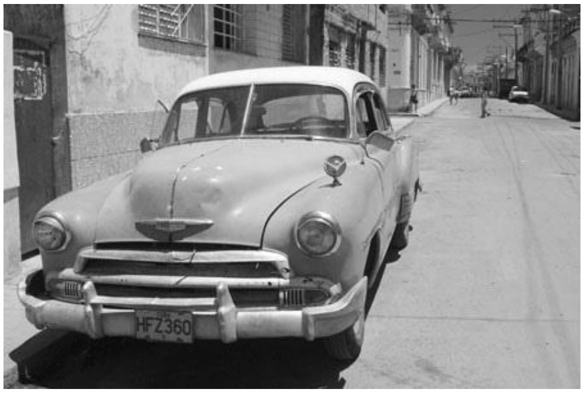

Figure 8: Image before Watermarking (450 x 300)

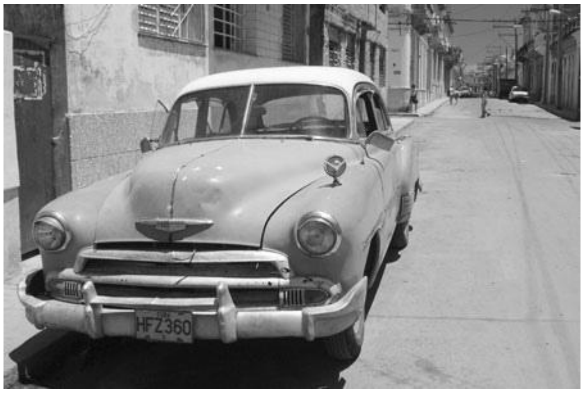

Figure 9: Image after watermarking (*Watermarked2*)

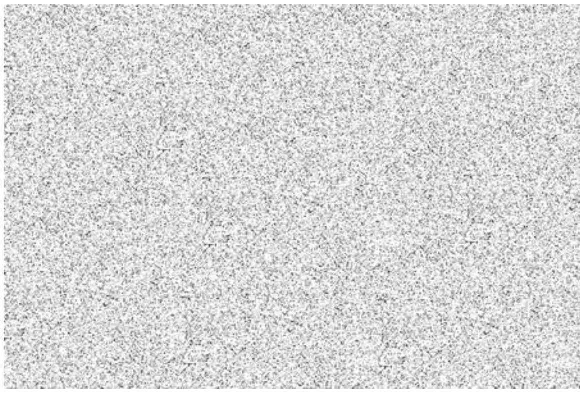

Figure 10: Difference of images (original and watermarked)

We used a 450x300 gray-scale image and performed this method. First, we took watermark1 as shown in figure 6. This watermark1 is encrypted and then this encrypted watermark is embedded into another watermark (here referred as watermarked watermark) as shown in figure 7. Now, this watermarked watermark is embedded into the main image. Figure 8 shows the original image before watermarking and figure 9 shows the image after watermarking. The difference between original and the watermarked image is shown above in figure 10.

V. CONCLUSION

In this paper, a new technique of digital watermarking is proposed in which a watermark is encrypted and embedded into another watermark and this combined watermark is embedded into the main image. This phenomenon of embedding one watermark into another is known as Nested watermarking. By doing so, the level of security of the watermark increases (due to use of encryption and decryption techniques) and the embedding capacity of the watermark is also enhanced (as concept of nested watermarks is used). The Blowfish encryption and decryption algorithm is used in this method as it is suitable and efficient for hardware implementation. Besides, it is unpatented and no license is required (Open source algorithm).

Advantages of this proposed method:

- Concept of Nesting increases embedding capacity of watermark into the main image.
- Encryption of watermarks before embedding them into main image helps to increase the security of the watermark.
- Use of Blowfish algorithm helps to make the method more robust.

FUTURE SCOPE

The concept of digital watermarking is not very matured. A lot of research is going on for improving the existing watermarking techniques. In this field, the highest priority is given to the work that is initiated towards getting information from attacked watermarks. The watermarking technique proposed in this paper can be improvised in future in terms of enhancing security and embedding capacity of watermarks. In this paper, we have used Blowfish Algorithm for encryption and decryption and LSB method for embedding of watermarks. So in future, some other algorithms can be used or proposed for encryption or decryption and embedding of watermarks.

REFERENCES

[1] Dobsicek, M., Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[2] 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.

[3] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, “Data Hiding in Binary Image for Authentication and Annotation”, IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004 Page(s): 528 – 538.

[4] Harpuneet Kaur, R. S. Salaria, “Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data”, The IASTED International Conference on Communication, Network, and Information Security (CNIS–2006), MIT, Cambridge, Massachusetts, USA, Oct 9–11, 2006. (Communicated)

[5] 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.

[6] Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, “Data Embedding Based on Better Use of Bits in Image Pixels”, International Journal of Signal Processing Vol 2, No. 2, 2005, Page(s): 104 – 107.

[7] 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.

[8] S.K.Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, PoulumiDas, "A Secure Scheme for Image Transformation", August 2008, IEEE SNPD, Page(s): 490 – 493.

[9] Mohammad ali, Moh'd Bani Younes, "An approach to enhance image encryption using blockbased transformation algorithm".

[10] G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic.

[11] Irfan.Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary, "Image encryption and decryption using blowfish algorithm " 2012 ,World Journal of Science and Technology.

[12] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[13] 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.

[14] MEENA V. KAMBLE, "INFORMATION HIDING TECHNOLOGY- A WATERMARKING", Advances in Computational Research, ISSN: 0975–3273, Volume 3, Issue 1, 2011, PP-37-41

[15] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3, ISSN 2249-6343.

[16] Kundur, Hatzinakos, Towards "Robust Logo Watermarking using Multiresolution Image Fusion principles" , IEEE Transactions on Multimnedia, vol. 6, no. 1, pp. 185-198, February 2004.

[17] Shah Kruti R., Bhavika Gambhava, "New Approach of Data Encryption Standard Algorithm" , International Journal of Soft Computing and Engineering (IJSCE) ,ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[18] Pankaj Rakheja, "Integrating DNA Computing in International Data Encryption Algorithm (IDEA)", International Journal of Computer Applications (0975 – 8887) Volume 26– No.3, July 2011

[19] Patterson and Hennessy, "Computer Organization & Design: The Hardware/ Software Interface", Morgan Kaufmann, Inc. 1994.

[20] Frank Hartung, Martin Kutter, "Multimedia Watermarking Techniques", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103, July 1999.

[21] Biermann, Christopher J. (1996). "7". *Handbook of Pulping and Papermaking* (2 ed.). San Diego, California, USA: Academic Press. p. 171. ISBN 0-12-097362-6..

AUTHORS

First Author – Jasdeep Singh Bhalla, Student, B.Tech, Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, jasdeepbhalla@gmail.com.
Second Author – Preeti Nagrath, Asst. Professor, Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, preeti.nagrath@bharatividyapeeth.edu