Digital Watermarking using Spatial Domain and Blowfish Algorithm

Piyoosh Pandey[1], Manish Gupta[2]

[1]Department of Computer Science, United College of Engineering and Research, Allahabad

[2]Department of Information Technology, United College of Engineering and Research, Allahabad

[1]piyush.pandey.off@gmail.com, [2]manish25may@rediffmail.com

***Abstract*— Use of internet in open environment in today's era, introduces the new set of problems of copyright protection, security and authentication of digital images. This paper is about the robustness of a digital watermarking scheme to protect and authenticate digital images. The process starts with a goal of gaining high level of privacy and efficiency by combining digital watermarking with symmetric key cryptography together to embed the secret information. By using a secret key Blowfish algorithm generates an encrypted watermark to embed it within a cover image. Embedding an encrypted watermark in spatial domain of cover image makes it very difficult for invaders to access and alter the images. The experimental results from MATLAB implementation of proposed scheme indicate the good imperceptibility, capacity and robustness against various noise attacks. The possible applications for the proposed scheme are content protection, copyright protection, message authentication and data integrity.**

***Keywords*— Blowfish, Copyright, Cryptography, Digital Watermarking, Privacy, Spatial Domain.**

I. INTRODUCTION

The increase in sharing of multimedia data over the protected and unprotected [5] networks makes security of data a primary concern. Cryptography is a science of information security [6] and it deals with the designs of encryption & decryption algorithms to ensure the secrecy and/or authenticity of messages [6]. Encryption is the process of encoding a message into ciphertext with a key whereas decryption is decoding that ciphertext into message with a key. In the symmetric key algorithm same secret key is used for both encryption and decryption of message. With the use of symmetric key algorithm we can encrypt a digital image to create encrypted watermark image. By the use of digital watermarking information related to copyright protection can be embedded into the cover image after making changes in its spatial domain. To extend the level of data security and authenticity, cryptography and digital watermarking can be combined together. Digital watermarking is embedding the copyright information in the body of media by making changes in its domain to ensure the authenticity of the message. A combined approach of cryptography and digital watermarking provides a solution to secure the digital images over the communication network. We have applied the combined approach of digital watermarking with the symmetric key cryptography on digital images to provide security and authentication. Blowfish is a secret-key block cipher. The block size is of 64 bits, and the key can be of any length up to 448 bits [2].

II. LITERATURE REVIEW

A robust watermarking scheme based on wavelet transform proposed by *Kundur and Hatzinakos* [4]. The scheme is about decomposing both the original image and the cover image up to L level. The original un-watermarked image is required because this is an informed technique.

An image encryption algorithm based on pixels proposed by Zhu *et al.* [9]. First, the image is encrypted by pixel scrambling, then add watermark to the scrambled image and at last a camouflaged image to vision or the pixels of the interactive image [6]. ECC is used to encrypt the core parameters to provide a new access to satisfy high level security [6].

A watermarking algorithm proposed by *Nirupma Tiwari et al.* [8] to protect digital data in which the embedding watermark is encrypted by DES (Data Encryption Standard) algorithm which is strong against various attacks. On the original image two level DWT (Discrete Wavelet Transformation) is applied.

A robust watermarking scheme proposed by *Manish Gupta and Dharmendra Kumar* [5], in which symmetric key algorithm (DES) is used to encrypt original image to produce the encrypted watermark. The encrypted watermark image embedded into the cover image by using spatial domain technique [5]. The performance metrics were Peak Signal to Noise Ratio (PSNR), Normalized Cross Correlation (NCC) and Image Histograms in the proposed scheme.

Mudita Srivastava *et. al.*[6], proposed a robust watermarking scheme by using Triple DES as symmetric key algorithm because DES is not sufficient and vulnerable to brute force attack in today's computing power [6]. In this scheme original image is encrypted by TDES using a secret key bundle to produce encrypted watermark image that embedded into the spatial domain of cover image.

In this paper we have proposed a robust digital watermarking scheme by using spatial domain technique for gray scale and colour images in which a gray scale image is encrypted with the Blowfish algorithm to produce the encrypted watermark image. The encrypted watermark image embedded into the cover image by using spatial domain digital watermarking technique and a colour image is decomposed into Red, Green and Blue (RGB) components. After decomposition the process used for the gray scale image applied separately on the Red, Green and Blue components. To recover the original image inverse process is applied. The recovered original image is identical to the original image. The performance of the proposed scheme is estimated on the basis of PSNR and NCC metrics.

III. SYMMETRIC KEY CRYPTOGRAPHY AND DIGITAL WATERMARKING

The scheme starts with selection of original image and cover image. Digital watermarking techniques are basically of two types: Spatial domain and Transform Domain. The watermarking techniques with the use of transform domain were developed earlier. This work use the Spatial domain of watermarking technique because of its advantages of easy implementation, less complexity, high capacity & better imperceptibility [6]. By using Blowfish algorithm we can produce a secure and robust encrypted watermark image from the original image to embed it into the spatial domain of cover image. There is an important role of embedding coefficient for extraction of the watermark of satisfying visual quality [6]. Knowing the embedding coefficient is essential to carry out extraction process [6].

In 1993, Bruce Schneier published the Blowfish block cipher [7] as free and fast alternative of symmetric key algorithm. Blowfish algorithm encrypts the 64 bit plaintext block by using variable length key from 32 bit to 448 bit. It is fast encryption algorithm among the existing cryptographic algorithm. It is a Feistel network, iterating a simple encryption function 16 times. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [2]. The algorithm consist of two parts, first one is key expansion and second is the data encryption. For key expansion and encryption a P-array consist of 18 32 bit subkeys P1, P2,…, P18 [2] and the four 32-bit S-boxes with 256 entries in each S-box [2] are used. For decryption process is same as encryption but the sub-keys Pi (i=1 to 18) must be supplied in reverse order [7].

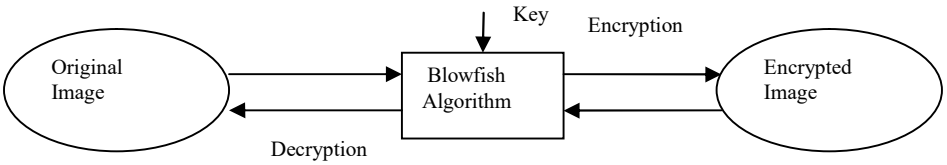

Fig. 1 Blowfish Encryption and Decryption

With the Blowfish algorithm sender encrypts the original image to produce the encrypted watermark after choosing a secret key. The digital watermarking scheme helps to embed the encrypted watermark image into the spatial domain of cover image to produce the embedded cover image. The sender sends the embedded cover image to the receiver. The receiver receives the embedded cover image and extracts the encrypted watermark image from it by using spatial domain digital watermarking extraction method. The extracted encrypted watermark image then decrypted by using the Blowfish decryption algorithm with the help of same secret key used by sender to encrypt the original images. The receiver must know the secret key to decrypt the extracted encrypted watermark image. After decryption of the extracted encrypted watermark receiver finds the recovered original image. The recovered original image is identical to the original image.

A. Digital Watermarking Scheme for Gray Scale Images

1) Encryption and Extraction Scheme for Gray Scale Images: In the first step gray scale original image and gray scale cover image are selected. Sender chooses a secret key to encrypt the image. With the use of Blowfish algorithm sender encrypts the original image which is the encrypted watermark image on sender side. The encrypted watermark image is embedded into the cover image to produce embedded cover image. For embedding the encrypted watermark spatial domain of the cover image is used.

2) Extraction and Decryption Scheme for Gray Scale Images: The receiver extracts the encrypted watermark image from received embedded cover image using spatial domain. The extracted encrypted watermark image is the watermark on receiver side. The extracted encrypted watermark image decrypted with blowfish algorithm by using same key used by sender to encrypt the image. The image obtained after decryption is the recovered original image. The recovered image is identical to the original image encrypted by sender.

B. *Digital Watermarking Scheme for Colour Images*

1) Encryption and Embedding Scheme for Colour Images: In the first step original colour image and colour cover image are selected. Sender splits the colour original image into Red, Green and Blue (RGB) images and chooses a secret key to encrypt all the images one by one by using Blowfish encryption algorithm to produce Red, Green and Blue encrypted watermark images. After encrypting the three RGB original images sender splits the colour cover images into Red, Green and Blue (RGB) cover images. The Red, Green and Blue encrypted watermark images are embedded into the spatial domain of Red, Green and Blue cover images respectively to form three Red, Green, Blue embedded cover images. The sender combines the three RGB embedded cover images into one embedded colour cover image. The sender sends the embedded colour cover images to the receiver. Fig.2 describes the encryption and embedding method for colour image.

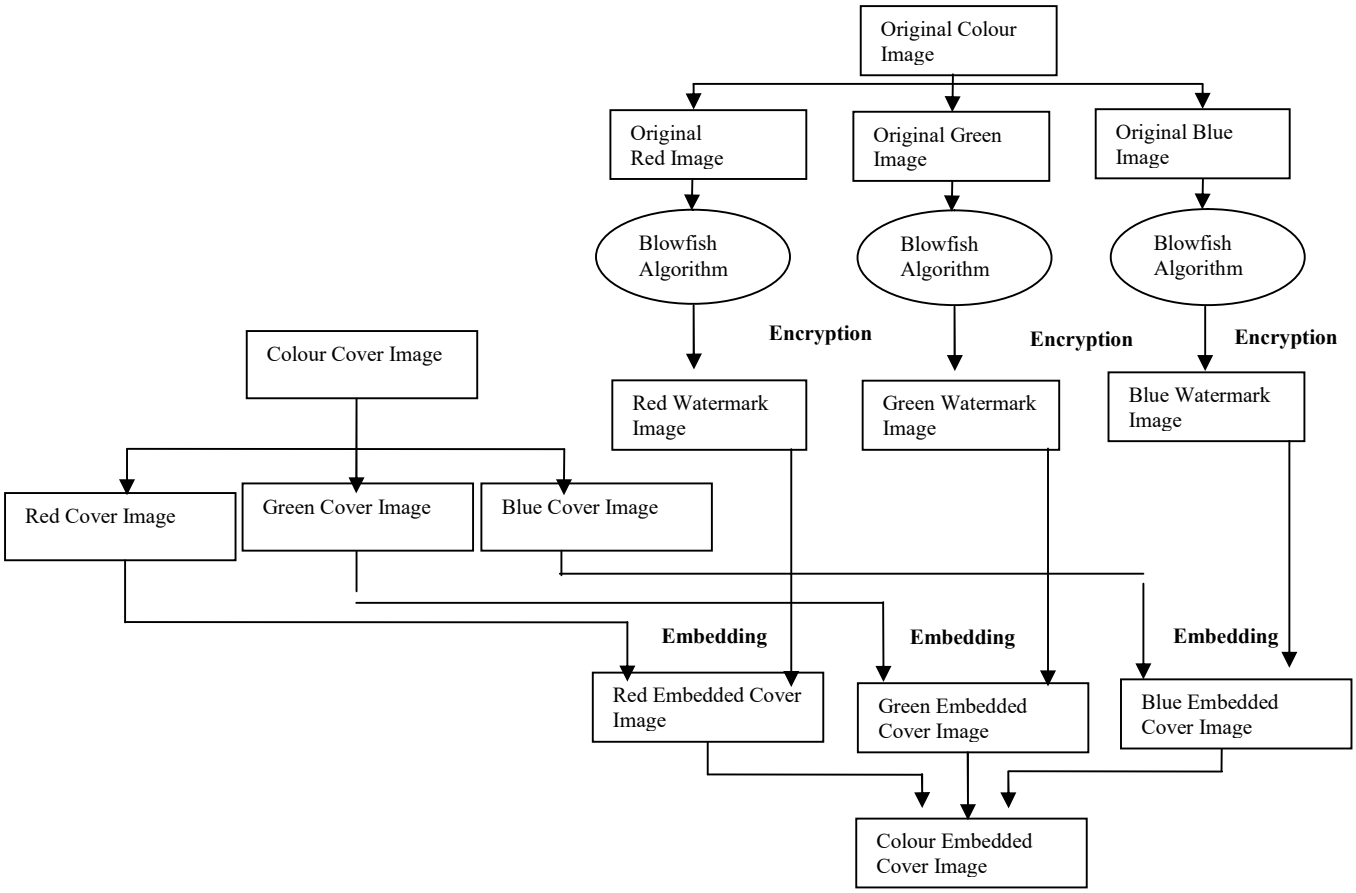

Fig. 2 Digital Watermarking Encryption and Embedding Scheme for Colour Image

2) Extraction and Decryption Scheme for Colour Images: The receiver splits the received colour embedded cover image into Red, Green and Blue (RGB) embedded cover images and extracts the three Red, Green and Blue encrypted watermark images from it by using the spatial domain. The three Red, Green and Blue extracted encrypted watermark images then decrypted one by one with Blowfish decryption algorithm by using the same secret key used by sender to encrypt the original image. The three recovered Red, Green and Blue images are combined to produce the recovered colour image. The recovered colour image is identical to the original colour image encrypted by the sender. Fig. 3 describes the Extraction and Decryption method for colour image.

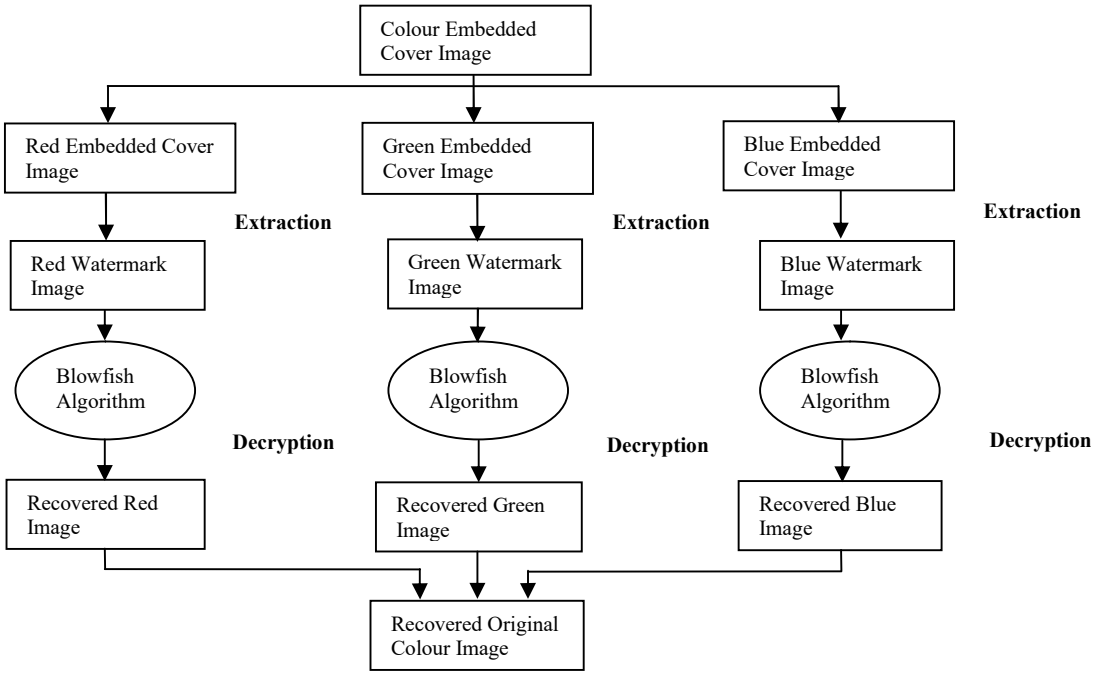

Fig. 3 Digital Watermarking Extraction and Decryption Scheme for Colour Image

IV. EXPERIMENT AND RESULT SIMULATION

For the simulation of proposed scheme on MATLAB, a BMP colour image of size 64x64 (shown in Fig.4(a)) is taken as the original image and a BMP colour image of size 512x512 (shown in Fig.4 (h)) taken as the cover image to embed the original image. The original colour image split into three RGB images. Fig. 4(b), 4(c) and 4(d) shows the original Red, Green and Blue images. Fig. 4(e), 4(f) and 4(g) shows the Red, Green and Blue encrypted watermark images. The colour cover image split into three RGB cover images. Fig. 4(i), 4(j) and 4(k) are the Red, Green and Blue cover images. After embedding the encrypted watermarks images into the cover images Fig. 4(m), 4(n) and 4(o) shows the Red, Green and Blue embedded cover images. The combined RGB embedded cover images results a colour embedded cover image shown in Fig. 4(l). The Red, Green and Blue extracted encrypted watermark images from RGB embedded cover images shown in Fig. 4(p), 4(q) and 4(r) and Fig. 4(t), 4(u) and 4(v) shows the recovered Red, Green and Blue images obtained after decryption of the RGB extracted encrypted watermark images. The recovered Red, Green and Blue images combined to obtain the recovered original image shown in Fig. 4(s).

Fig. 4(a) Original Colour Image

Fig. 4(b) Original Red Image

Fig. 4(c) Original Green Image

Fig. 4(d) Original Blue Image

Fig. 4(e) Red Watermark Image

Fig. 4(f) Green Watermark Image

Fig. 4(g) Blue Watermark Image

Fig. 4(h) Colour Cover Image

Fig. 4(i) Red Cover Image

Fig. 4(j) Green Cover Image

Fig. 4(k) Blue Cover Image

Fig. 4(l) Colour Embedded Cover Image

Fig. 4(m) Red Embedded Cover Image

Fig. 4(n) Green Embedded Cover Image

Fig. 4(o) Blue Embedded Cover Image

Fig. 4(p) Red Extracted Watermark Image

Fig. 4(q) Green Extracted Watermark Image

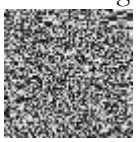

Fig. 4(r) Blue Extracted Watermark Image

Fig. 4(s) Recovered Colour Image

Fig. 4(t) Recovered Red Image

Fig. 4(u) Recovered Green Image

Fig. 4(v) Recovered Blue Image

Fig. 4 Result Simulation Images

The implementation of proposed scheme is evaluated on different performance metrics. The performance metrics are PSNR (Peak Signal to Noise Ratio) and NCC (Normalized Cross Correlation).

1) ***PSNR:*** It is a measurement of quality between two images. In this context we compare the quality of original cover image and embedded cover image. From 0 to 100 dB is the resultant value and optimal value is ≥ +35dB [6].

2) ***NCC:*** It is to check the quality between original image and recovered original image. From -1.0 to 1.0 is the resultant value and optimal value is 0.85 ≤ 1.0 [6]. The NCC with noise calculated between the original image and the image recovered from embedded cover image after adding different types of noises into the embedded cover image.

The images shown in samples are for 64x64 size BMP colour images implementation. For gray scale image the proposed scheme directly applied on a 64x64 size BMP gray scale image without using the split mechanism as colour image. The proposed scheme results compared with the results of scheme proposed by *Manish Gupta and Dharmendra Kumar* [5] for performance evaluation.

TABLE I
RESULT

Symmetric Key Algorithms	Metrics	Noises	Images			
			Gray Scale	Colour		
				Red	Green	Blue
Blowfish	PSNR		+63.17dB	+62.95dB	+63.09dB	+63.25dB
	NCC	*Without Noise*	1.0000	1.0000	1.0000	1.0000
		Poisson	0.5431	0.0102	-0.0141	0.0168
		Speckle	0.5320	0.0101	0.0026	-0.0095
		Gaussian	0.5437	0.0175	-0.0034	0.0106
		Salt & Pepper	0.6142	0.1332	0.1734	0.1332
DES[5]	PSNR		+63.17dB	+62.85dB	+63.07dB	+63.25dB
	NCC	*Without Noise*	1.0000	1.0000	1.0000	1.0000
		Poisson	0.5346	0.0125	0.0105	0.0078
		Speckle	0.5385	0.0094	-0.0153	-0.0172
		Gaussian	0.5526	-0.0048	-0.0011	0.0042
		Salt & Pepper	0.6330	0.1179	0.1760	0.1311

V. CONCLUSION

In this work blowfish algorithm is used to encrypt a digital image to generate encrypted watermark image. The watermark embedded in the cover image by using spatial domain technique of digital watermarking. The contribution of the work is to provide a robust and fast digital watermarking scheme to ensure high capacity, secrecy and robustness against various noises added to the digital images. We have applied the proposed scheme on gray scale and colour images on PNG and BMP file formats. By the experimental results we can see that our proposed scheme provides good imperceptibility, capacity and robustness against different noises on digital images.

REFERENCES

[1] A. Forouzan, Behrouz, 2007, Cryptography & Network Security, New Delhi, Tata McGraw-Hill.

[2] 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.

[3] B. Schneier, "The Blowfish Encryption Algorithm – One Year Later", Dr. Dobb's Journal, September 1995.

[4] Deepa Kundur and Dimitrios Hatzinakos. "A robust digital image watermarking method using wavelet-based fusion." In icip, pp. 544-547. IEEE, 1997.

[5] Manish Gupta and Dharmendra Kumar, "Design and Implementation of Digital Watermarking using Symmetric Key Cryptography (Data Encryption Standard)", Germany, Lambert, 2014.

[6] Mudita Srivastava, H M Singh, Manish Gupta, Dharm Raj, "Digital Watermarking using Spatial Domain and Triple DES," 2016 International Conference on Computing for Sustainable Global Development (INDIACom), March 16-18, 2016, pp. 3031-3035. IEEE, 2016

[7] Pia Singh,Prof. Karamjeet Singh, "IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB," International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013. ISSN 2229-5518.

[8] Nirupma Tiwari, Manoj Kumar Ramaiya, and Monika Sharma. "Digital Watermarking using DWT and DES." In Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp. 1100-1102. IEEE, 2013.

[9] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang, and Mengmeng Wang. "Digital image encryption algorithm based on pixels." In Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on, vol. 1, pp. 769-772. IEEE, 2010.
[10] Schneier on Security: The Blowfish Encryption Algorithm.[Online]. Available: https://www.schneier.com/academic/blowfish.