Asian Journal of Information Technology 15 (23): 4820-4827, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Curvelet Transform Based Visible Colour Image Watermarking Technique Using VLSI

[1]M. Senthilkumar and [2]P.S. Periasamy
[1]Department of Electrical and Electronics Engineering, K.S.R College of Engineering
637215 Tiruchengode, India
[2]Department of Electronics and Communication Engineering, K.S.R College of Engineering
637215 Tiruchengode, India

Abstract: Due to rapid development in the network and communication field, it has become necessary to protect the data 0during transmission. Digital watermarking is a solution to the copyright protectionand authentication of data in the network. This study aims to prevent unauthorized duplication of image and to transmit confidential image. By this way hackers will not suspect the existence of secret information. Conventional methods having information loss during recovery, it will be easily hacked, lower embedding capacity, requires more memory and power consumption. The proposed scheme offers an effective protection, data embedding along with high security. Curvelet transform and inverse curvelet transformare performed andthenvisible logo isembedded on colour image. For transferring confidential data, a content owner encrypts the original uncompressed colour image using an encryption key and then image-hider will compress the LSB ofeach pixel of all three planes in the encrypted colour image using an image-hiding key to create a space to hold secret image. In order to extract secret image and to recover the original content simultaneously both image hiding key and encryption key are necessary. Lower memory requirements, speed of encryption and randomization in encryption key generation are improved by parallel RC4 algorithm. Hidden image security will be increased by odd and even shuffling of secret image bits within compressed encrypted colour image. It has good embedding capacity and better quality recovered image than conventional methods.

Key words: Curvelet transform, RC4, private keys, stream cipher, encryption, cryptography, watermarking.

INTRODUCTION

Due to rapid development in communication and network areas it has become necessary to prevent confidential data from illegal hackers, for this purpose information hiding will be used.Information hiding means communication of information by hiding and retrieving from any digital media. Information hiding is a general term encompassing three disciplines namely cryptography, watermarking and steganography. Watermarking hides the copyright information into the digital media through certain algorithm. The digital media are image, an audio, a video or simply a plain text file. The secret information to be embedded will be some confidential text, author's serial number, company logo, images with some special importance. The watermark is hidden in the digital data either visibly or invisibly. Cryptography is most often associated with scrambling plaintextinto cipher text this process is called encryption and vice versa known as decryption.

There are also a number of works on data hiding differs on method used for data embedding. In (Anumol *et al*., 2013), cover image and secret images are converted to vector form, then to decimal form. Secret image is embedded in the LSB of cover image. Then the image isprocessed using the simulink block sets which read an image in bit by bit format. The elliptic curve cryptography method presented in (Chitla and Mohan, 2012) authenticates the information by generating signature and signed messages. In (Gunjal, 2011), scrambled watermark is embedded in middle frequency sub band and Arnold Transform is used to scramble the image. In (Devapriya and Ramar, 2010), (Sandeep and Rajiv, 2013) embedding method is multiplicative, done at second level of DWT decomposition is most favorable choice of the embedding strength. In data embedding is done on LSBmodification of cover image,embed the watermark bits in the blocks located at the even columns in the HL region of an image and the blocks located at the odd columns in the LH region of an image. In (Umaamaheshvari and Thanushkodi, 2012), multiple binary watermarks are embedded into digital medical image based on the concept

Corresponding Author: M. Senthilkumar, Department of Electrical and Electronics Engineering, K.S.R College of Engineering, 637215 Tiruchengode, India

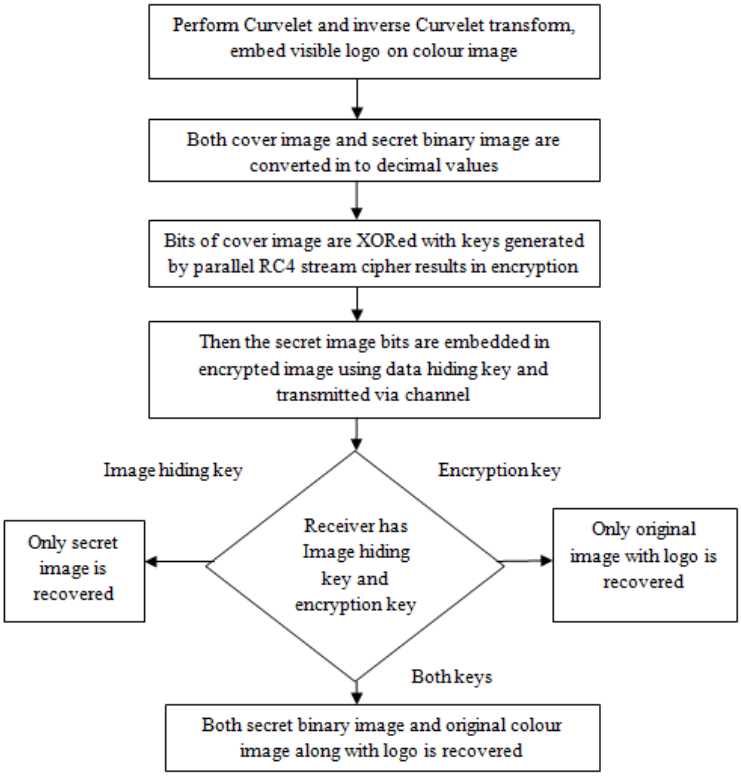

Fig. 1: Process involved in watermarking and information hiding

of visual cryptography. Reversible data hiding method presented in (Manikandan *et al*., 2012; Ni *et al*., 2006; Zhang, 2011) uses data hiding key and encryption key if any one of key is lost both original image and secret data will lost. In separable reversible data hiding method presented by Zhang (2012) though receiver has lost encryption key will able to extract hidden data and if data hiding key has lost it is not possible to extract secret data but using encryption key alone original image will be recovered. In presence of both data hiding key and encryption key, receiver will decrypt image and recover original data simultaneously. Here, grayscale image is used as cover image and invisible watermarking has done.

Proposed method employ image as media for watermarking, both visible and invisible watermarking is used. Curvelet transformand inverse curvelet transform is performed on the colour image. Then, logo is embedded on colour image, it results in formation of visible watermarked image. Then, to transmit secret information, image is first encrypted and secret image in form of bits are embedded in LSB of encrypted colour image. Here, secret information are in form of binary images. In order to increase embedding capacity three binary images are hidden inside the encrypted colour image. First binary image is embedded in R plane ofencrypted image, second binary image is embedded on G plane ofencrypted image and third binary imageis embedded on B plane of encrypted image.Entire process is carried out in spatial domain it uses LSB of the image for embedding. Encryption (Gupta, 2012) is done on the image prior to secret image embedding. Encryption/decryption use proportioned keys generated by parallel RC4 stream cipher. It uses private key method for secret image extraction. Process involved in watermarking and information hiding as shown in Fig. 1.

MATERIALS AND METHODS

Colour image of size P1×P2 is taken as cover image, apply Curvelet and inverse Curvelet transform to the cover image. Then logo is embedded on cover image. Then three secret images are embedded in three planes of colour image namely RGB planes. Then visible watermarked image is converted into decimal values using MALAB 7.14 tool. After this confidential images are hidden inside the watermarked image. For image hiding three processes are to be carried out namely image encryption, secret image embedding and image-extraction using Modelsim 6.3f tool. The content owner encrypts the original uncompressed colour image using an encryption

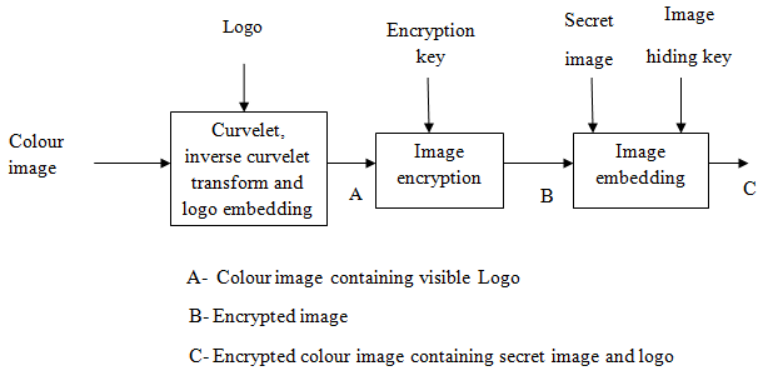

Fig. 2: Block diagram of transmitter

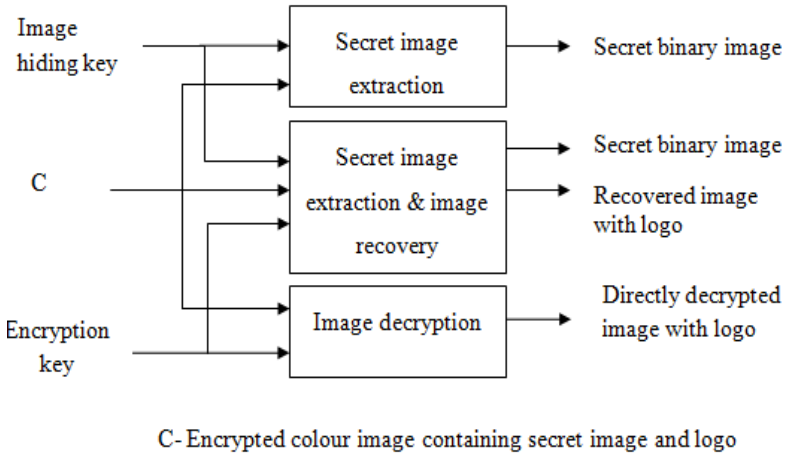

Fig. 3: Proposed separable scheme at the receiver

key to produce an encrypted image. Then, the image hider compresses the least significant bits (LSB) of each pixel inthe encrypted colour image using an image-hiding key to create a sparse space to accommodate the secret binary image Fig. 2.

At the receiver side, secrete image embedded in the created space will be easily retrieved from the encrypted image containing secret image according to the image hiding key. Since the image embedding affects the LSB not MSB of pixels, a decryption with the encryption key will result in an image similar to the original version. When using both of the encryption and image-hiding keys, the embedded additional secret image will be successfully extracted and the original image is perfectlydecrypted by exploiting the spatial correlation in natural image. If the receiver has encryption key alone will decrypt the image but not possible to extract secret image and if receiver has image hiding key alone will able to extract secret image not possible to decrypt image. Figure 3 shows proposed separable scheme at the receiver.

Visible watermarked image is encrypted by simply XOR the pixel value of image with keys generated by parallel RC4 stream cipher:

$$B_{i,j,u} \oplus = b_{i,j,u}\ r_{i,j,u} \quad (1)$$

Where:

$b_{i,j,u}$ = Pixels value of the of original image,

$r_{i,j,u}$ = The random keys generated by parallel RC4 (Mousa and Ahmad, 2006), (Kundan, 2013)

Parallel RC4 generate two keys per clock cycle and it is a stream cipher. $B_{i,j,u}$ are pixels value of encrypted image. Number of keys generated for encrypting the visible watermarked image is equal to the number of pixel in a watermarked image. Encryption keys which are generated by parallel RC4 are random and independent. Random keys which are used for encryption process is symmetric with random keys used for decryption process. It follows a private mode of encryption.

Secret image embedding: For embedding secret image, select P_n encrypted pixels of P encrypted pixels from R plane of encrypted colour image. Repeat this procedure for G and B planes of encrypted colour image, results in three groups of P_n encrypted pixels are used to carry the parameters for image hiding. P_n is the positive integer denotes group of pixels which carriesthe values of D, M, V.P is the total number of pixel in an watermarked image. The LSB of ($P-P_n$) encrypted pixels of RGB planes are compressed and divided into a number of groups each group contains M pixels. For each pixel-group, collect the D least significant bits of the M pixels and denote them as B (k, 1), B (k,2), ..., B (k, M×D) where k is a group index within [1, ($P-P_n$) /M] and D denotes number of bits selected from each pixel of an single group and it is a positive integer<5. The image-hider generates a matrix G sized ((D×M-V) ×D×M) for three planes of colour image individually, So three G sized matrix are generated which is composed of two parts:

$$G = [ID.M.VQ] \tag{2}$$

In Eq. 2 the left part is an (D×M-V) × (D×M-V) identity matrix, the right part Q sized (D×M-V)V is a pseudo-random binary matrix (Zhang, 2012) derived from the image-hiding key. Then, embed the values of the parameters D, M and V into the LSB of P_n selected encrypted pixels corresponding to RGB planes.

Finally, total of ($P-P_n$)×V/M bits made up of P_n original LSB of selected encrypted pixels and ($P-P_n$)×V/M-P_n additional bits will be embedded into the pixel groups.($P-P_n$)×V/M pixel group of RGB plane are multiply with G matrix:

$$\begin{pmatrix} B'(k,1) \\ B'(k,2) \\ . \\ . \\ B':(k,D\cdot M-V) \end{pmatrix} = G.\begin{pmatrix} B(k,1) \\ B(k,2) \\ . \\ . \\ B(k,D.M) \end{pmatrix} \tag{3}$$

Where: the arithmetic is modulo-2 By (3), B (k,1), B (k,2),...,B (k, D×M) are compressed as B'k,1), B' (k,2),...,B' (k, D×M-V) and a sparse space is therefore available for secret image accommodation. In D×M-V space, secret image bits are embedded. Since colour image is used as cover these procedure is applied to R plane, G plane, B plane individually.

Let B' (k,D×M-V+1), B' (k,D×M-V+2),..., B'(k,D×M) of each group be the original LSB of selected encrypted pixels and the additional data to be embedded. Then, replace the B (k, 1), B(k,2),...,B (k, D×M) with the new B' (k, 1), B '(k,2),...,B' (k, M×L) and put them into their original positions by an inverse permutation. At the same time, the (8-D) Most Significant Bits (MSB) of encrypted pixels are kept unchanged. Since V bits are embedded into each pixel-group, the total ($P-P_n$)V/M bits will be accommodated in all groups of colour image. While embedding secret image bits, odd bits are embedded in one group and even bits are embedded in another group. By this way security is increased. The embedding capacity(EC) is:

$$EC = 3\times\frac{V}{M} \tag{4}$$

Where:

M = The number of pixel in each group

V = The number of bits embedded in each group

Secret image extraction and image recovery: During image recovery and secret image extraction three cases are possible, that the receiver has only the image hiding key only the encryption key and both the image hiding and encryption keys as shown Fig. 3. With an encrypted image containing embedded secret image, if the receiver has only the image-hiding key will obtain the values of the parameters D, M and V from the LSB of the $P_n$selected encrypted pixels. The receiver permutes and divides the other ($P-P_n$) pixels into (P-Pn)/M groups and extracts the V embedded bits from the D LSB-planes of each group. When having the total ($P-P_n$)V/M extracted bits, the receiver will divide them into (P-Pn) original LSB of selected encrypted pixels and ($P-P_n$) V/M-P_n additional bits.

Suppose the receiver has encryption key means only original image content along with Logo will be recovered. Denoting the bits of pixels in the encrypted image containing embedded image as $B'_{i,j.0}$, $B'_{i,j,1}$,...$B'_{i,j,7}$ ($1\le i\le P1$ and $1\le j\le P2$) the receiver will decrypt the received data as (Zhang, 2011):

$$b'_{i,j,u} = B'_{i,j,u} \oplus r_{i,j,u} \tag{5}$$

In Eq. 5, $b'_{i,j,u}$ are pixel values of decrypted image, $r_{i,j,u}$ are derived from the encryption key generated by parallel RC4 stream cipher which generates two keys per clock cycle. Calculate average energy of distortion (AE) as in (Zhang, 2012) is:

$$AE = \frac{(2^V - 1)}{2^V} 2^{-2D} \sum_{\alpha=0}^{2^D-1} \sum_{\beta=0}^{2^D-1} (\alpha - \beta)^2 \quad (6)$$

In Eq. (6) α and β is original imageand decrypted image respectively. The value of Peak Signal to Noise Ratio (PSNR) in the directly decrypted image is

$$PSNR = 10\log_{10}(AE) \quad (7)$$

If the receiver has both the image-hiding and the encryption keys will extract the embedded image and recover the original image. According to the image-hiding key, the values of D, M and V, the original LSB of the P_n selected encrypted pixels and the (P-P_n) V/M-P_n additional bits are extracted from the encrypted image containing embedded image. By putting the P_n LSB into their original positions, the encrypted image of the P_n selected pixels are retrieved three planes of colour image and their original intensity values are correctly decrypted using the encryption keys. To recover the original intensity values of the other (P-P_n)pixels, Consider a pixel-group because B'(k,1), B'(k,2),...B'(k,D×M-V) in Eq. 3 are given and $[B (k,1), B (k,2), .. B (k,M)]^T$ must be one of the vectors meeting (Zhang, 2012):

$$S = [B' (k,1), B' (k,2),....B' (k,M L-S)00..0] T + a.H \quad (8)$$

Equation 8, a is an arbitrary binary vector sized 1×V and H is an V× DM matrix made up of the transpose of Q and an V×V identity matrix

$$H = [Q^T I_V] \quad (9)$$

Equation 10 denoting the decrypted pixel-group as Gk and the intensity values in it as $t_{i,j}$, then calculate the total difference between the decrypted and estimated intensity values (Zhang, 2012) in the all group of RGB planes:

$$di = \sum_{(i,j)\in Gk} \left| t_{i,j} - \tilde{p}_{i,j} \right| \quad (10)$$

where, the estimated intensity values ($\overline{p_{i,j}}$) is generated from the neighbors in the directly decrypted image:

$$\overline{p_{i,j}} = \frac{\left[p'_{i-1}/2^D\right] + \left[p'_{i+1}/2^D\right] + \left[p'_{i,j-1}/2^D\right] + \left[p'_{i,j+1}/2^D\right]}{4} 2^D + 2^{D-1} \quad (11)$$

By Eq. 11, the estimated pixel values as by Zhang (2012) are only dependent on the MSB of neighbor pixels. Mean Square Error (MSE) is calculated using following:

$$MSE = \frac{\sum_{i=1}^{512} (error)^2 \Big/ (512)^2}{512} \quad (12)$$

Similarity Ratio (SR) is calculated using following Eq. 13:

$$MSE = \frac{\text{Maximum similar data}}{\text{Total data}} \quad (13)$$

RESULTS AND DISCUSSION

The test colour image Lena of size 512×512 as shown in Fig. 4a is used as cover image in this experiment. Curvelet and inverse curvelet transform is performed initially. After that logoof size 128×128 was embeddedon cover image results in visible watermarking. Then watermarked image is encrypted using encryption key. For information hiding information in form of binary image (camera man) of size 185×185 is written as bits in LSB of each pixel in the encrypted image using image hiding key. Fig. 4e. Encrypted watermarked image containing secret binary image with embedding capacity of 0.399. To decrypt the image and to recover the hidden binary image two keys are necessary as shown in Fig. 4g. If receiver has image hiding key will recover binary image but decryption of image. If the receiver has encryption key will decrypt the watermarked image but not possible to extract hidden binary image as shown in Fig. 5f. The papua forest destruction image taken by satellite of size 512×512 as shown in Fig. 6 and 7a is used as cover image in this experiment. Curvelet and inverse curvelet transform is performed initially. After that logo of size 128×128 was embeddedon cover image results in visible watermarking. Then, watermarked image is encrypted using encryption key. For information hiding information in form of binary image (camera man) of size 185×185 is written as bits in LSB of each pixel in the encrypted image using image hiding key. Figure 6e encrypted watermarked image containing secret binary image with embedding capacity of 0.399. To decrypt the image and to recover the hidden binary image two keys are necessary as shown in Fig. 6g. If receiver has image hiding key will recover binary image but decryption of image is not possible. If the receiver has encryption key will decrypt the watermarked image but not possible to extract hidden binary image as shown in Fig. 6f. Table 1 shows experimental results of

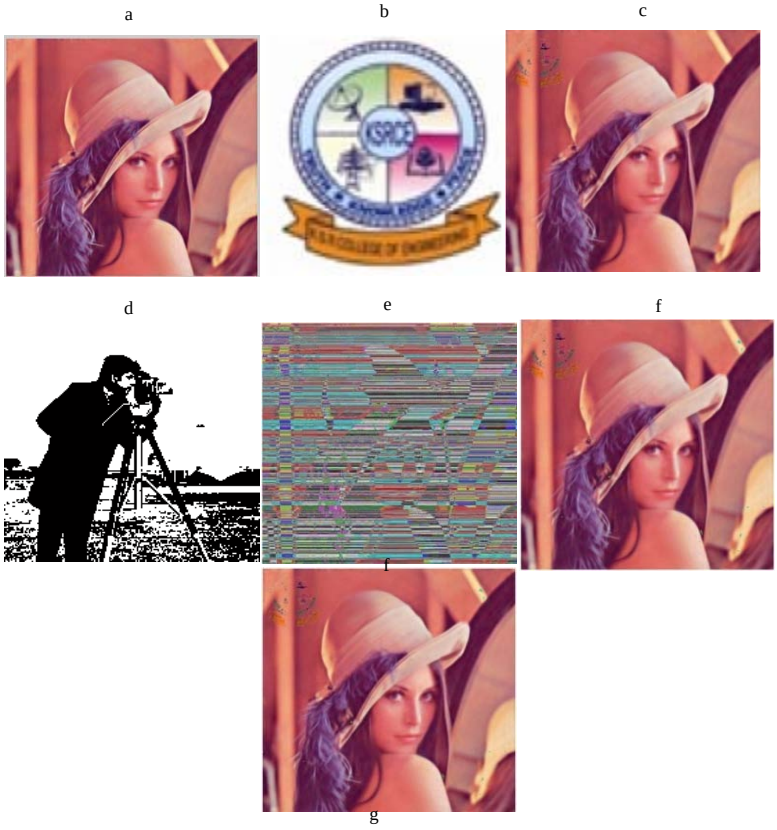

Fig. 4: a) Cover image of size 512×512; b) Logo of size 128×128; c) Watermarked image; d) Secret binary image of size 185×185; e) Encrypted watermarked image containing secret binary image with embedding capacity of 0.399; f) Directly decrypted image (only encryption key) with PSNR 36.7dB and g) Recovered image (encryption key and image hiding key) with PSNR 45.06 dB

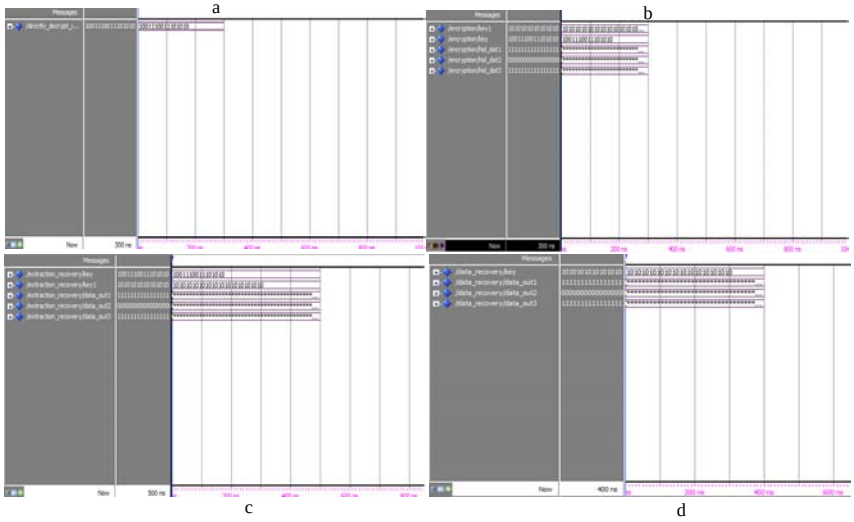

Fig. 5: Modelsim simulated waveform: a) Output for encryption of lena image; b) Output for directly decrypted image using encryption key alone; c) Output of decryption of image and secret image recovery using encryption key and image hiding key, respectively and d) Output of secret image recovery using image hiding key

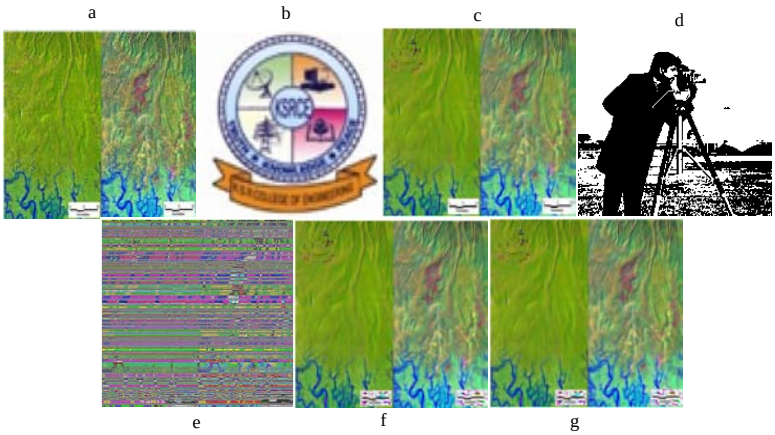

Fig. 6: a) Satellite image of papua forest destruction is taken as cover image of size 512×512; b) Logo of size 128×128; c) Watermarked image; d) Secret binary image of size 185×185; e) Encrypted watermarked image containing secret binary image with embedding capacity of 0.399; f) Directly decrypted image (only encryption key) with PSNR 40.24dB and g) Recovered image (encryption key andimage hiding key) with PSNR 42.57 dB

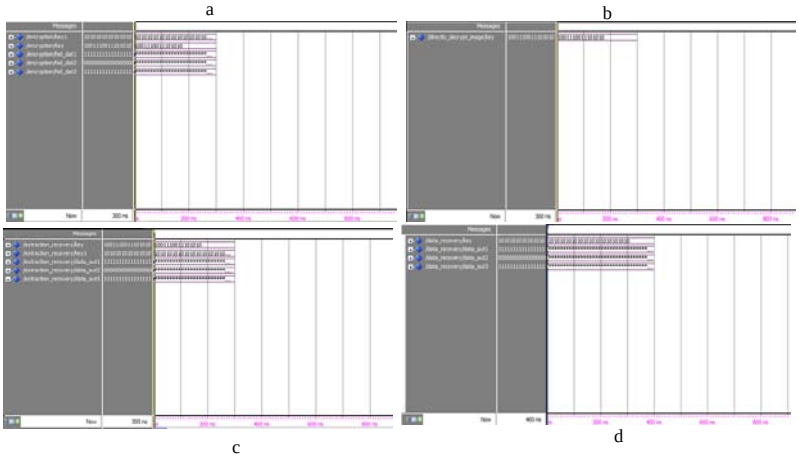

Fig. 7: Modelsim simulated waveform; a) Output for encryption of papua forest destruction; b) Output for directly decrypted image using encryption key alone; c) Output of decryption of image and secret image recovery using encryption key and image hiding key respectively and d) Output of secret image recovery using image hiding key

Table 1: Experimental results of reversible method and proposed separable scheme applied for different colour images

	Reversible method (using two keys)				Proposed separable method Directly decrypt (encryption key)				Ecovered image key a Rnd image hiding key)			
Type of image	PSNR	MSE	SR	EC	PSNR	MSE	SR	EC	PSNR	MSE	SR	EC
Lena image	39.65	0.037	0.166	0.062	36.70	0.024	0.257	0.399	45.06	0.024	0.266	0.399
Airplane image	44.51	0.013	0.156	0.062	35.53	0.010	0.252	0.399	45.43	0.010	0.273	0.399
Baboon image	40.26	0.013	0.158	0.062	34.88	0.006	0.257	0.399	44.33	0.006	0.243	0.399
Satellite image of the salina porto ingles.	47.01	0.959	0.148	0.062	43.48	0.905	0.240	0.399	48.37	0.905	0.255	0.399
VLSI die layout image	51.25	0.75	0.125	0.062	52.74	0.640	0.160	0.399	53.49	0.640	0.156	0.399
Niagara falls image	43.41	0.152	0.138	0.062	36.37	0.134	0.262	0.399	45.30	0.134	0.238	0.399
Satellite image of papua forest destruction	37.95	0.423	0.222	0.062	40.24	0.380	0.274	0.399	42.57	0.379	0.265	0.399
Trapezium star cluster image in the orion nebula infrared camera	40.25	0.233	0.125	0.062	40.51	0.113	0.233	0.399	42.31	0.113	0.266	0.399

proposed scheme applied for different colour images. Separable method is applied to various colour image and resultsof directly decrypted(image hiding key) images are compared with recovered images (both image hiding key and encryption key).

CONCLUSION

The proposed scheme offers an effective protection, data embedding along with high security. It offers authentication by curvelet transform based visible watermarking and allows secret transmission of image within cover image. For transferring confidential image, a content owner encrypts the original uncompressed colour image using an encryption key. Then image hider may compress the LSB of all three planes of encrypted colour image using image-hiding key for embedding secret image. Though the receiver has lost any of the two keys it is either possible to extract secret image or to decrypt image. Lower memory requirements, speed of theencryption process and randomized encryption key generation are improved by parallel RC4 algorithm. Hidden image security has increased by odd and even shuffling of secret image.

RECOMMENDATIONS

In future the processed image will be implemented in FPGA to calculate power, memory requirements etc and extend to apply this concept from image to video.

IMPLICATIONS

With the conception of separable encrypted watermarking on colour image, the identification and copyright ownership protection are carried out. Digital content embedded with watermarks depicting metadata identifies the copyright owners. It plays a vital role in military application where the secret transmission of confidential data issignificant.

REFERENCES

Anumol, T.J., V.A. Binson and S. Rasheed, 2013. FPGA implementation of low power, high speed, area efficient invisible image watermarking algorithm for images. Intl. J. Sci. Eng. Res., 4: 1-6.

Chitla, A. and M.C. Mohan, 2012. Authentication of images through lossless watermarking (LWM) technique with the aid of elliptic curve cryptography (ECC). Intl. J. Comput. Appl., 57: 17-25.

Devapriya, M. and K. Ramar, 2010. Statistical image watermarking in DWT with capacity improvement. Global J. Comput. Sci. Technol., 10: 20-24.

Gunjal, B.L., 2011. Wavelet based color image watermarking scheme giving high robustness and exact corelation. Intl. J. Emerging Trends Eng. Technol., 1: 21-30.

Gupta, P., 2012. Cryptography based digital image watermarking algorithm to increase security of watermark data. Int. J. Sci. Eng. Res., 3: 1-4.

Kundan, M., 2013. A new robust enrichment symmetric stream cipher approach for confidentiality based on rc4 stream cipher algorithm. Intl. J. Eng. Res. Technol., 2: 1-8.

Manikandan, R., M. Uma and S.M. MahalakshmiPreethi, 2012. Reversible data hiding for encrypted image. J. Comput. Appl., 5: 104-110.

Mousa, A. and A. Hamad, 2006. Evaluation of the RC4 Algorithm for Data Encryption. IJCSA., 3: 44-56.

Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol., 16: 354-362.

Sandeep, K. and B. Rajiv, 2013. Enhanced technique for watermarking using MFHWT. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 1199-1202.

Umaamaheshvari, A. and K. Thanushkodi, 2012. A novel watermarking technique based on visual cryptography. Intl. J. Adv. Res. Comput. Eng. Technol., 1: 70-74.

Zhang, X., 2011. Reversible data hiding in encrypted image. IEEE. Signal Process. Lett., 18: 255-258.

Zhang, X., 2012. Separable reversible data hiding in encrypted image. Trans. Inform. Forensics Secur., 7: 826-832.