Improved the Security Strength of Visual Cryptography using Feature based Watermarking Technique

Sandeep Singh Baghel
Department of Information Technology
SATI
Vldisha (M.P) India

Ajay Goyal
Department of Information Technology
SATI
Vldisha (M.P) India

ABSTRACT
Data integrity and confidentiality is major issue in internet based communication. For the integrity and confidently used various cryptography and stenography technique. The traditional message hiding technique faced a problem of intruder. The intruder easily decrypts the image and gets information. For the improvement of security strength used various key cryptography technique for hiding of information. In consequence of data hiding visual cryptography is another milestone. The process of visual cryptography used technique of share generation for the authentication of image. The process of share generation used mathematical formula and derivations. In this paper proposed feature based watermarking technique for visual cryptography. The feature based process used two feature property of image, color and texture feature. The color feature property generates a key value and texture feature property generates the value of share for the visual cryptography. The proposed method is simulated in MATLAB software and applies some geometrical attack for the measuring of security strength.

General Terms
Visual Cryptography, Watermarking, Geometrical Attack Share Generation

Keywords
Watermarking, cryptography, generation of Key

1. INTRODUCTION
The concept of share generation in visual cryptography proposed by Nair and Shamir in 1995[1, 2]. The proposed visual cryptography technique encodes the digital image into number of image using nosing process. The share based image has greater advantage over the traditional steaganography technique. The strength of security is increase in concern of geometrical and some other intruder based attack. The process of share generation used the technique of image pixel expansion for cryptography purpose. The major drawback of pixel based share generation is distortion of share. If the generated share is distorted, image can't be recovered. In journey of visual cryptography used various techniques and improved the security strength [4, 5]. The grid based visual cryptography and many more techniques. The feature based visual cryptography is new area of research in the field of cryptography and steaganography. In feature based visual cryptography used the lower content of features of image such as color, texture. The dominated color features are used for the generation of key for the hiding an information. The texture feature is used for the generation of shares. The texture feature is important feature of any digital image. For the extraction of texture feature used discrete wavelet transform function. The wavelet transform function is well known texture feature descriptor. The wavelet transforms function used 2D transform for the extraction of feature. The extracted feature generates the share for the hiding of image information. For the generation of key used color model [15]. The HSV color model used here for the combination of key generation to The HSV color model used two level random key generation process for the authentication. Share era for the visual cryptography should likewise be possible by the idea of watermarking utilizing some watermarking strategy. We can utilize these watermarked offers for recovering the shrouded data. This exertion can create the significant shares as opposed to a few shares having no data. In this paper used water making based concept for visual cryptography. The watermarking process generates a texture based share and encrypts the image. The rest of paper discuss as in section 2 discuss the key generation technique. In section 3 Discuss the share generation technique .in section 4 discuss proposed method. In section 5 discuss experimental result analysis and finally discuss conclusion & future work in section 6.

2. KEY GENERATION
Generation of key is important phase of visual cryptography. The generated key gives the authentication process of embedding of image by share. For the generation of key used HSV color model. The HSV color model has three color component hue, saturation and value. All three components converted into binary format and apply the randomization algorithm for the formation of session key. The session key is the component of input image. The generation of key used XOR operation for the final key generation [14]. The generated key used for the embedding of share for the visual cryptography.

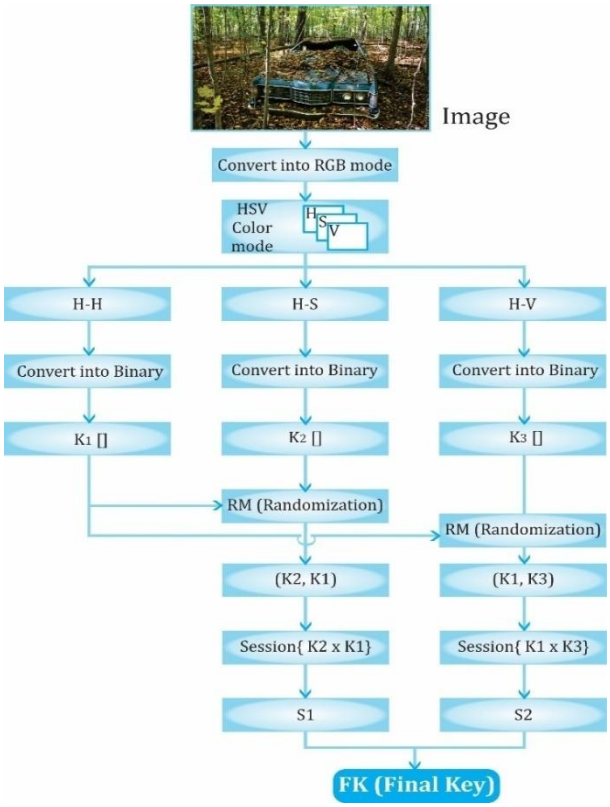

Figure 1 block diagram of key generation based on HSV color model

3. SHARE GENERATION

In this section disucss the process of share generation based on DWT(2) transfrom function. The DWT(2) transfrom function gives the texture feature of given image. The estimate of texture features depends of approxiamte part of image. The value of approximate part is compostion of low pass filter. The value of high pass ffilte prserve in terms of details. The value of transfrom gives the texture transparent pixel data for the genration of share. The generation of share coccourence value of detail component. The level of dtails creates the share part of transfrom fiunction. The texture feature of input image denoted by P1,p2,….pn. and the details coefficent is denoted by d1,d2,…….dn. the compotion of (p,d) creates the number of level of share. The transfrom function apply 2D transfrom creates 8 share and apply 4 creates 16 share and increase the number of share accoridng to the level of transfrom function. The generation of share describe in block diagram.

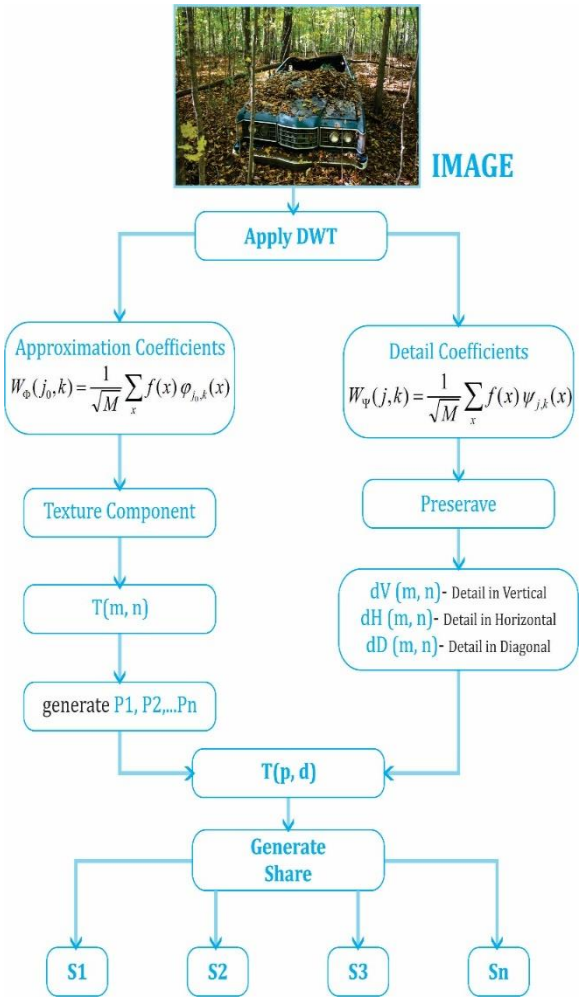

Figure 2 block diagram of share genration based on DWT(2) transfrom function

4. PROPOSED ALGORITHM

The proposed algorithm of visual cryptography is a combination of wavelet based share generation and HSV based key generation. The key and share encrypt the image for the visual cryptography. The generation of share depends on the level of transform function. The process of share generation already describes in section III. And share used key for the encryption process. The generation of key also discuss in section II.

Procedure of DWT (2)

Begin

The process of transform gives number of shares

The total number of share generates according to the level of transform

Do

Share (P, D)

Estimate details component

While (D (m, n)>P (m, n))

Share= level of transform function

End

Call key value ()

If (share = 0)

{Go to DWT (2)

}

Else

Encrypt the share along with image

If (level! =0)

{Call key value ()

}

Else

Embedding the image

Apply geometrical attack and measure the parameter for security strength.

5. EXPERIMENTAL RESULT

The proposed algorithm implemented in MATLAB software. And used standard image dataset for the generation of share and watermarking of image. For the estimation of security strength apply various geometrical attacks. For measuring of performance used PSNR and NC. The analysis of result given in table and graph are.

Table 1 shows the comparative PSNR and NC for Barbara image on the basis RCVC method.

Types of Attack	White Noise Attack	Gaussian Noise Attack	JPEG Compression Attack	Transform Attack	Cropping Attack	Decoding Attack
PSNR	50.1575	70.9659	40.5286	42.52168	44.5189	36.2288
NC	0.9975	0.9782	1	0.8702	0.4709	1

Table 2 Shows the comparative PSNR and NC for Barbara image on the basis Proposed method.

Types of Attack	White Noise Attack	Gaussian Noise Attack	JPEG Compression Attack	Transform Attack	Cropping Attack	Decoding Attack
PSNR	54.3587	32.4181	34.5272	45.5164	39.5193	48.0246
NC	0.9997	1	1	0.8702	0.3857	1

Table 3 shows the comparative PSNR and NC for Historical image on the basis RCVC method.

Types of Attack	White Noise Attack	Gaussian Noise Attack	JPEG Compression Attack	Transform Attack	Cropping Attack	Decoding Attack
PSNR	65.5584	81.7818	22.3644	32.359	42.3627	51.7591
NC	0.9996	0.9993	1	0.8346	0.3848	1

Table 4 Shows the comparative PSNR and NC for Historical image on the basis Proposed method.

Types of Attack	White Noise Attack	Gaussian Noise Attack	JPEG Compression Attack	Transform Attack	Cropping Attack	Decoding Attack
PSNR	86.0932	70.8216	42.3641	32.3589	52.3631	66.1775
NC	1	0.9785	1	0.8346	0.4828	1

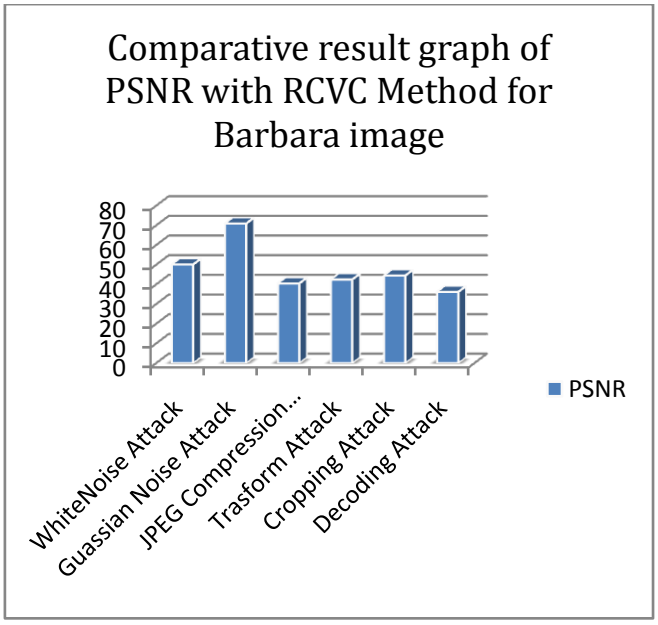

Figure 3: Shows that the comparative result for Barbara image using RCVC methods, here we find the value of PSNR for their respective types of attacks.

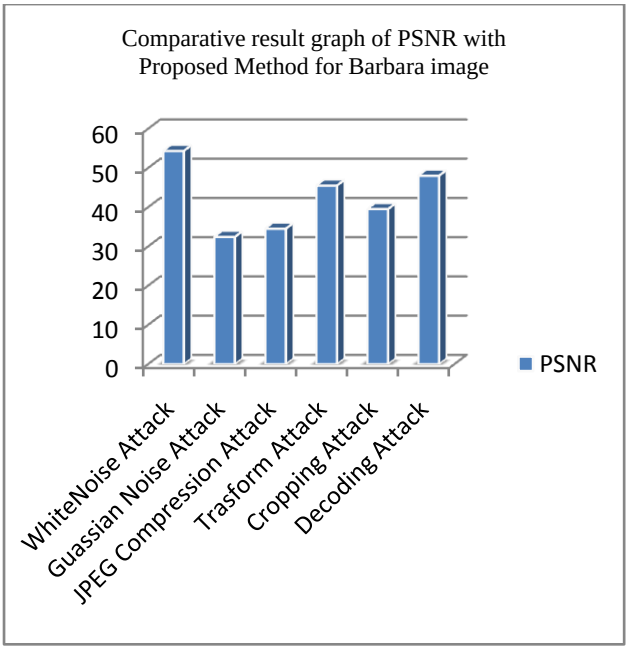

Figure 4: Shows that the comparative result for Barbara image using proposed methods, here we find the value of PSNR for their respective types of attacks.

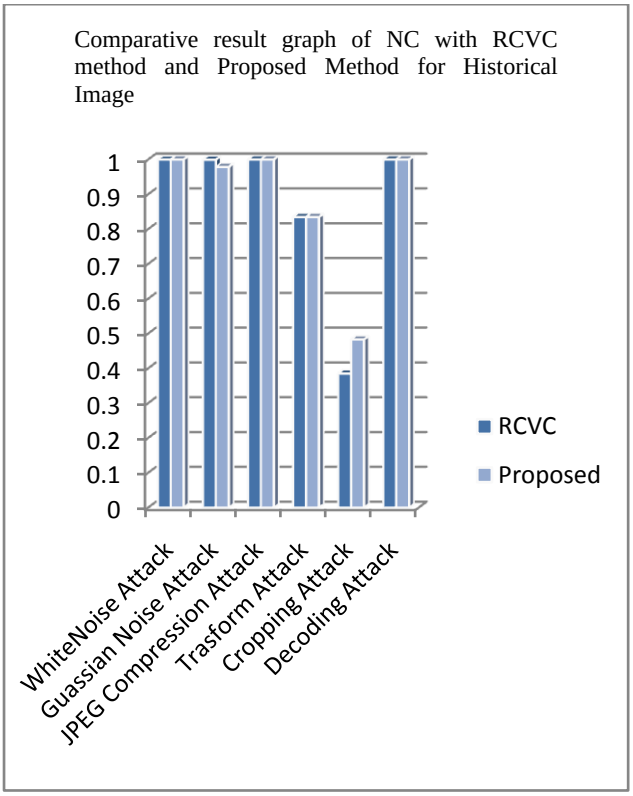

Figure 5: Shows that the comparative result for Historical image using RCVC and Proposed methods, here we find the value of NC for their respective types of attacks.

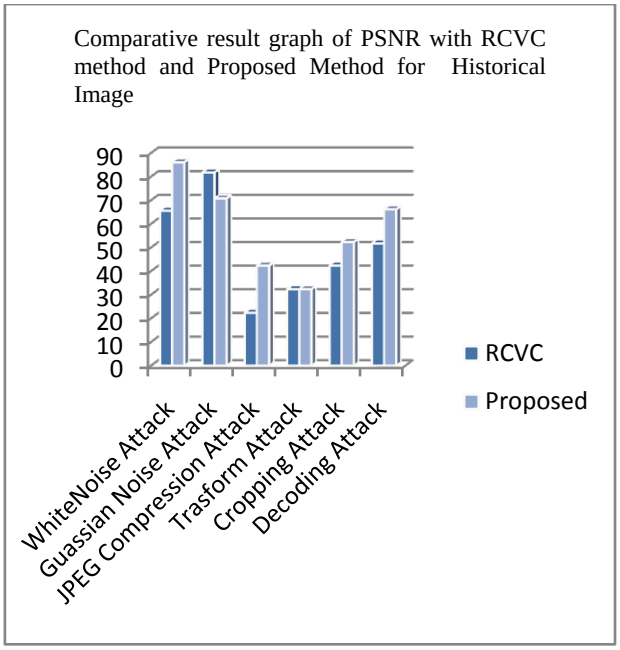

Figure 6: Shows that the comparative result for Historical image using RCVC and Proposed methods, here we find the value of PSNR for their respective types of attacks.

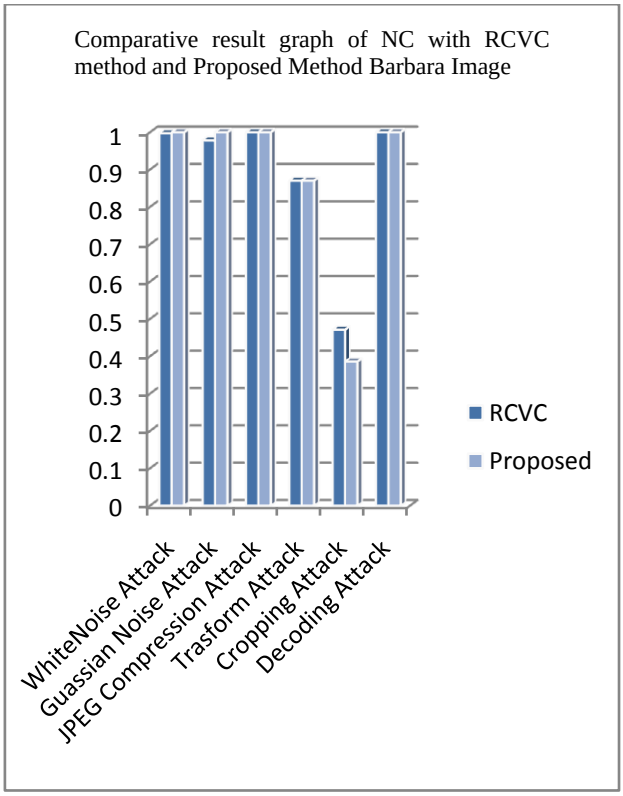

Figure 7: Shows that the comparative result for Barbara image using RCVC and Proposed methods, here we find the value of NC for their respective types of attacks.

6. CONCLUSION AND FUTURE WORK

In this paper proposed a novel method for visual cryptography based on share generation and key authentication. For the generation of share used DWT (2) transform function. The generated share represents the texture feature of given image and controlled by the details part of transform function. For the generation of key used HSV color model. For the

generation of key used HSV color model. HSV has three components in form of color hue, saturation and value. These values are randomized and binaries create session key. In session key apply the XOR operation and finally gets value of key for the process of encryption. The generation of maximum number of shares depends on the value of transform function. For the validation of proposed algorithm used MATLAB software and apply some geometrical attack and measure the security strength of cryptography technique. In the process of analysis used two parameters one is PSNR and other is NC. The value of PSNR indicates the quality of image and the value of NC is measure the correlation strength of shred embedded image. For the comparative analysis used another visual cryptography technique such as RCVS. The proposed algorithm is very robust in terms of NC and quality of image. The strength of proposed algorithm reduces the possibility of intruder attack. In future used real time scenario and also tested on different domain of transform function.

7. REFERENCES

[1] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin "Random-grid-based Visual Cryptography Schemes" IEEE, 2013, Pp 1-12.

[2] Kai-Hui Lee and Pei-Ling Chiu "Sharing Visual Secrets in Single Image Random Dot Stereogram's" IEEE, 2014, Pp 4336-4348.

[3] Xiaotian Wu, Duanhao Ou, Lu Dai, Wei Sun "XOR-Based Meaningful Visual Secret Sharing by Generalized Random Grids" IH&MMSec, 2013, Pp 181-191.

[4] Gayathri Soman, Mr. Jyothish K John "Secure Digital Image Sharing Using Diverse Image Media" IJIACS, 2015, Pp 154-161.

[5] Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarka, Pp 98-113

[6] Juby Justin and Giss George "An Extented Vesual Cryptography algorithm for general Access Structures", ijaret, 2013, Pp 1-4.

[7] Anran Wang, Shuai Ma, Chunming Hu, Jinpeng Huai, Chunyi Peng, Guobin Shen "Enhancing Reliability to Boost the Throughput over Screen-Camera Links", IEEE, 2013, Pp 1-12.

[8] Bharanivendhan N and Amitha T "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm", International Journal of Computer Applications, 2014, Pp 11-16.

[9] Jun Kong, Omer Barkol, Ruth Bergman, Ayelet Pnueli, Sagi Schein, Kang Zhang, and Chunying Zhao "Web Interface Interpretation Using Graph Grammars" IEEE, 2012, Pp 590-602.

[10] Sian-Jheng Lin, Shang-Kuan Chen and Ja-Chen Lin "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion", Elsevier, 2010, Pp 900-916.

[11] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad "Mobile Phone Sensing Systems: A Survey", IEEE, 2013, Pp 402-427.

[12] J. Galbally "Biometric Antispoofing Methods: A Survey in Face Recognition", IEEE, 2015, Pp 1530-1552.

[13] Snehal N. Meshram and Sneha U. Bohra "Implementation of Random Grid Visual Cryptography for Color Images", IJSR, 2013, Pp 2545-2549

[14] Er.Supriya Kinger, "Efficient Visual Cryptography", Journal of emerging technology in web intelligent, Vol. 2, No. 2, 2010

[15] Barnali Gupta Banik and Samir Kumar Bandyopadhyay" Secret Sharing using 3 level DWT method of Image Steganography based on Lorenz Chaotic Encryption and Visual Cryptography" in International Conference on Computational Intelligence and Communication Networks 2015