An Efficient Image Watermarking for Combination of RST Attacks

Sheshang D. Degadwala
Research Scholar
Madhav University,
Rajasthan

Sanjay Gaur, PhD
Research Supervisor
Madhav University,
Rajasthan

ABSTRACT
Nowadays in network communication need to protect the transmission, also right to advance networking helpful fast Communication. Therefore, networking makers need to additional consistently handling illegal use of the data. In our proposed approach, first enter the user name and password then generate QR-code using zxing library that will converted in to the share using Binary Visual cryptography algorithm. Now share-2 is save in the database that is for future reference at receiver side. Now share-1 is embedding into the R-Component LL bit using of block DWT-SVD and Pseudo Zernike moment. After embedding add G, B Component. Now Color watermark image transfer from the network. As in network there are different attackers apply combination of Rotation, Scale and Translation attacks on the color watermark image. For recover the attacks first apply Pseudo Zernike moment, Surf feature on R-component they will extract the attacks pixel and recover the scale-angle using affine transformation. Now share-1 and another share-2 is in data base so we will apply EX-OR operation to get the QR-Code. The final QR-code is decoded and we get the user name and password. This research work can give a way for providing Security to Authority data and give protection against Attacks.

Keywords
QR Codes, VCS, RGB-Extract, Block-DWT, Surf, Affine and Combinational RST attacks.

1. INTRODUCTION
The enormous Growth in e-world which will be coupled for reality totally Web furthermore headway to machine execution encouraged the initial circulation of advanced information. Done globe totally Web because of rupture in security advanced picture camwood a chance to be undoubtedly duplicated and disseminated without straight reasonably. Those advanced watermarking schemes have been recommended will flexibility these sorts for unapproved right about advanced media information. Toward starting stage, encryption and control get systems are used to copyright protection, content verification Also proprietorship security. In any case presently days, the advanced watermarking strategies are utilized prominently on stay with advanced media secure [1] [2].

Watermarking may be an example about odds embedded under an advanced image, sound alternately feature record that identifies those files copyright majority of the data. The same advanced watermarking hails from the faintly noticeable watermark imprinted in stationary that identifies the maker of the stationary. The reason for the advanced watermarks may be will gatherings give copyright insurance for licensed innovation that's on advanced arrangement. [4] In this way watermark will be those concealed data inside the advanced indicator. There would a number requisitions for advanced watermarking Anyway Around the greater part copyright protection, substance authentication, duplicate and use control Furthermore content portrayal are imperative provision region of the advanced watermarking.

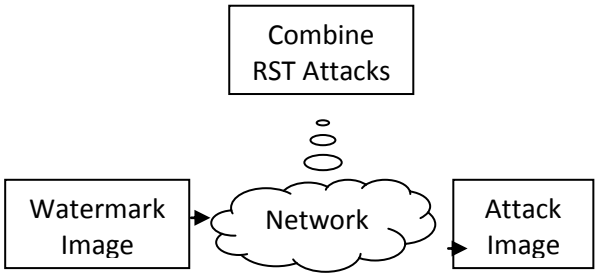

Fig 1: Network Scenario

Watermarking systems are arranged into spatial space techniques and change area strategies. Spatial area techniques are less unpredictable, however less strong against assaults. The watermarking plan in view of the change areas can be further divided into discrete wavelet transform (DWT) and discrete cosine transform (DCT), the discrete Fourier transform (DFT). Capacity of DWT-SVD based plan is more than DFT.

We have made system to do secure transaction which is visual cryptography scheme and, for copyright protection and deal with geometrical attacks the watermarking scheme is used. It's absolutely impossible that anybody could decode the data contained inside some of shares. At the point when the shares are stack together, decoding is conceivable when the shares are set more than each other. Now, the data turns out to be in a flash accessible. No additional computational power is required keeping in mind the end goal to decode the data.

2. RELATED WORKS

2.1 Visual Cryptography [22, 27, 29]
Visual cryptography may be a picture encryption technique, which protects picture built mystery. Visual cryptography doesn't oblige At whatever unpredictable calculation with unscramble the mystery image; Rather it could make carried out by human eyes through sight perusing which those immense profit from claiming utilizing visual cryptography. At present information security may be a Main mossy cup oak necessity similarly as it voyaged through web In Different networks? Different routines need been explored also created for better security from claiming our information. Mystery information might make in distinctive manifestations for example, such that image, audio, video, text, and so forth. Here our center will be main around picture built mystery. Visual cryptography assumes a key part in picture security. In the encryption procedure from claiming this system picture may be encrypted under numerous allotments Furthermore toward alternate hand ahead unscrambling side at or a

percentage of the stakes are stacked together will uncover the mystery picture. Diverse sorts about visual cryptography systems have been explored which may be customary visual cryptography, halftone visual cryptography, general get structure built visual cryptography, piece built progressive visual cryptography and irregular grid based visual cryptography, also as of late created hierarchic visual cryptography.

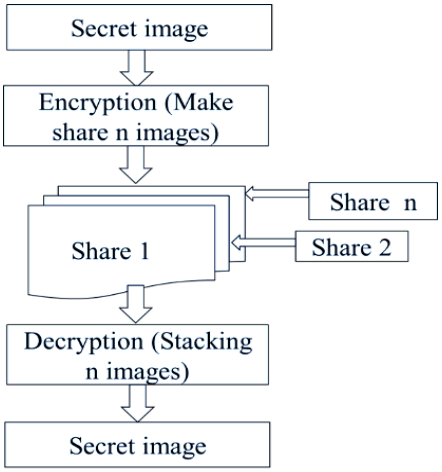

Fig 2: Visual Cryptography

In Decryption process all or qualified set of shares are required to be stacked together to reveal the secret. The encryption takes place in such a way so that at decryption side no mathematical equation is needed to decrypt the secret image. The original image which is to be encrypted is referred as secret image. Once the encryption is completed, ciphers are generated which is referred as shares. Share is a scramble form of original input image from single share anyone could not recover any idea about the original secret image. To share the secret among group of n participants is the fundamental idea behind visual cryptography [11].

There are 3 visual cryptographic schemes are available which is listed below:-

(A) visual cryptographic (2,2) scheme
(B) visual cryptographic (k, n) scheme
(C) visual cryptographic (n, n)scheme

Visual cryptographic (2, 2) scheme is basic scheme proposed by naor [1]. In this scheme the secret is separated into exactly two parts. These two shares must participate to reveal the secret. Another scheme, in which secret is encoded into n shares. To recover the original secret image both two shares are participate in decryption process. This scheme is known as 2 out of n- scheme.

2.2 Discrete Wave late Transformation (DWT) [6, 7]

Wavelet transform disintegrates a picture under an course of action about band compelled segments which could make reassembled to redo the principal picture without shortcoming since those information transmission of the ensuing coefficient sets is more diminutive over that of the 1st picture, those coefficient sets might make down inspected without reduction for information. Propagation cost of the 1st banner may be master toward up sifting, inspecting Also summing the individual sub gatherings. To 2-D pictures, applying DWT compares to get ready those picture toward 2-D channels previously, each estimation.

Those channels disconnect the information picture under four non-covering multi-determination coefficient sets, an easier determination estimation picture (LL1) Also even (HL1), verthandi (LH1) Furthermore inclining (HH1) point of interest segments seemed for figure. 5. The sub-band LL1 identifies with those coarse-scale DWT coefficients same time the coefficient sets LH1, HL1 What's more HH1 talk of the fine-size about DWT coefficients.

To get those accompanying coarser extent of wavelet coefficients, those sub-band LL1 is further took care of until a few completing up scale n will be come to. In the perspective At n may be attained we will need 3N+1 coefficient sets including of the multi-determination coefficient sets LLN What's more LHX, HLX and HHX the place x ranges starting with 1 until n.

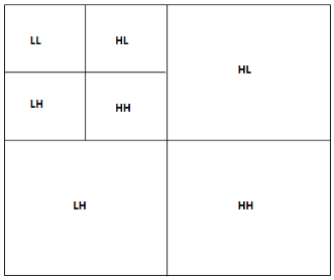

Fig 3: Decomposition model of DWT at level 2

At that point again, the helter skelter repeat coefficient sets HHx fuse those edges What's more surfaces of the picture and the mankind's eye will be not commonly fragile should progressions clinched alongside such coefficient sets. This permits the watermark with a chance to be embedded without being seen Eventually Tom's perusing the human eye.

2.3 SVD [9]

SVD is a standout amongst the most valuable apparatuses in direct variable based math with a few applications in picture pressure, watermarking, and other flag handling zones. In the event that an is a n×n network, then SVD of lattice A can be characterized as,

A = U*S*VT,……(1)

Where, U and V are the orthogonal networks and S is a corner to corner lattice. Askew components of S are the solitary qualities and they fulfill the accompanying property.

S (1,1) >S (2,2) >S (3,3) > . . . . . >S (n,n),…….....(2)

SVD will be great known to those watermarking done light of the certainty that few about singular qualities might talk with considerable section about banner vitality, SVD could a chance to be associated with square What's more rectangular pictures, the SV's of a picture bring extraordinary upheaval invulnerability, i. E. , SV's don't progress inside and out The point when An minimal inconvenience is included should An picture energy values, SV's talk will intrinsic scientific properties.

2.4 SURF [30]

Speeded Up Robust Features is a scale-invariant feature detector based on the Hessian matrix, as is, e.g., the Hessian-Laplace detector. However, rather than using a different measure for selecting the location and the scale, the determinant of the Hessian is used for both. The Hessian matrix is roughly approximated, using a set of box type filters, and no smoothing is applied when going from one scale to the next.

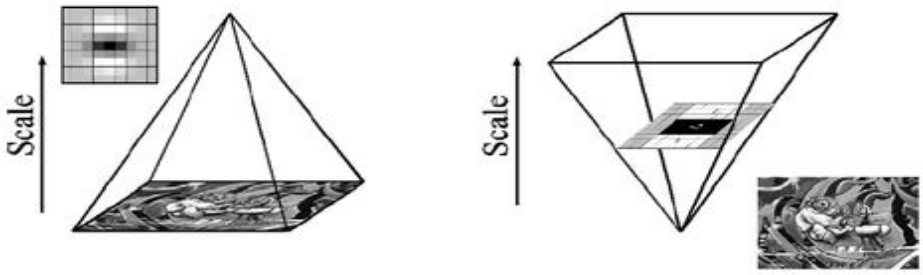

Fig 4: Surf Feature

Gaussians are optimal for scale-space analysis, but in practice they have to be discredited which introduces artifacts, in particular in small Gaussian Kernels. SURF pushes the approximation even further, using the box filters. These approximate second-order Gaussian derivatives, and can be evaluated very fast using integral images, independently of their size. Surprisingly, in spite of the rough approximations, the performance of the feature detector is comparable to the results Obtained with the discredited Gaussians. Box filters can produce a sufficient approximation of the Gaussian derivatives as there are many other sources of significant noise in the processing chain. SURF has been reported to be more than five times faster than DoG.

2.5 Pseudo Zernike moments [31]

Pseudo-Zernike polynomials are illustrious and broadly used in the exploration of optical schemes. Image analysis uses shape descriptors. PZM is geometric-based moment that uses the worldwide info in an image for extracting features. The orthogonal moments of PZM are shift, rotation, and scale invariants which are suitable for pattern recognition applications. Pseudo-Zernike contains several orthogonal sets of complex-valued polynomials defined as:

$$S_{rc}(X,Y) = R_{rc}(X,Y)\exp\left(jm\ \tan^{-1}\left(\frac{X}{Y}\right)\right), \ldots\ldots\ldots (3)$$

Where $X^2 + Y^2 \leq 1,\ r \geq 0, |c| \leq r.$

$$PZM_{rc} = \frac{r+1}{\pi}\sum X\ \sum Y\ f(X,Y)S_{rc}(X,Y) \ldots\ldots\ldots\ldots (4)$$

A=absolute (Z)

Angle (Z) = tan-1(imag(Z), real(Z));

Phi=angle (Z)*180/pie

It should be noted that the PZM is computed for positive m because $(x, y) = Vnm * (x, y)$. If an image is rotated, phase of moments in PZM will be varied and its absolute value remains constant. Thus, if the absolute value or value of PZM is considered as the feature, the feature f is independent of rotation [3]. Pseudo Zernike polynomials of order ≤P, contain

(+1)2 linearly independent polynomial of degree ≤ P.

Pseudo Zernike moment is used in optical system, pattern recognition and in image analysis as shape descriptors.

3. PROPOSED METHOD

After studying various visual cryptography schemes and watermarking schemes, we propose new technique for secure bank transaction. In this scheme we provide authenticity and data integrity of the shares using watermark technique. In our scheme we take one QR-image as original image or host image and create shares using 2-out-of-2 VC scheme [2]. When two shares will be created, server share is stored in bank database and client share is kept by user. The user will present with client share during all the transactions with bank. After that we apply the watermark technique on that client share image for providing the authentication and data integrity and send it on the open communication channel.

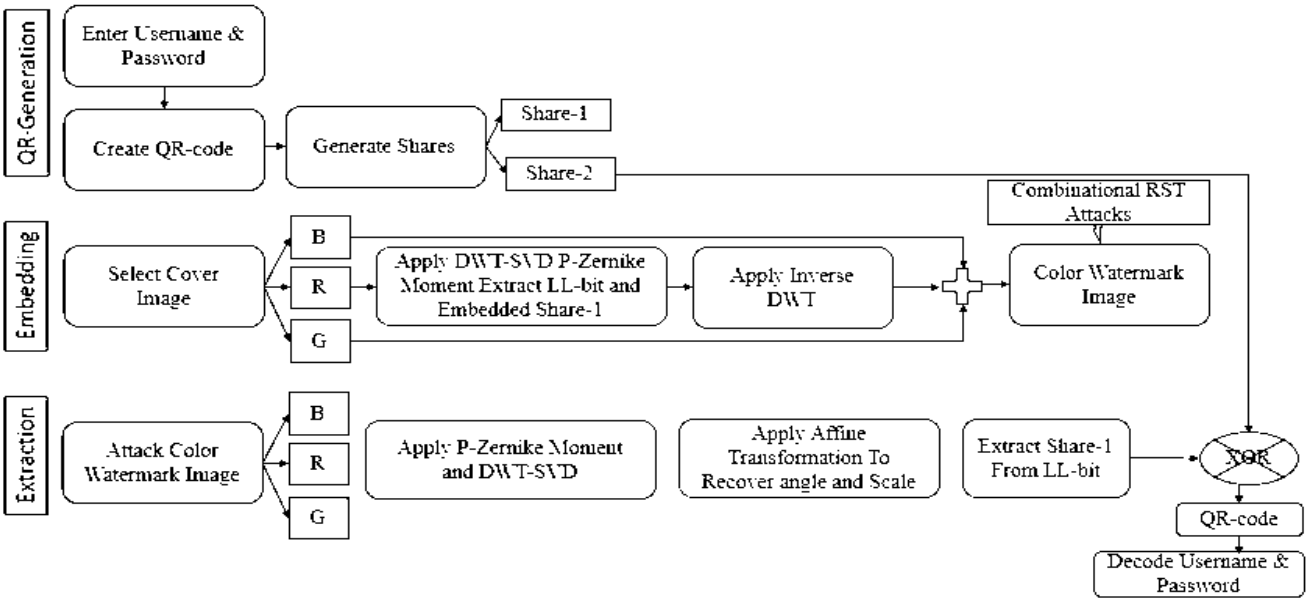

Fig 5: Proposed Block Diagram

QR-Generation: As shown in the Figure 2 First select the user name and password. Now using zxing library generating the QR-code. That QR-code is now in invisible form so now one can see the data inside. Further we have Apply VCS scheme to generate two shares of QR-Code.

Embedding: In this process as shown in the Figure 3 select the color cover image. Extract the R, G and B component. Now Select R-component and Apply P-Zernike Moment and DWT-SVD transformation and Extract LL-bit. In the LL-Bit embedding the Share-1 data. After Invers DWT-SVD transformation to generate R-Embedded Image Now Add Remain G and B Component to Create Color Water Mark

Image. Color Watermark Image is transmitted over the Network Different Attackers Apply RST attacks on it.

Extraction: After RST attacks getting the Attack Color Image Which is now apply the P-Zernike Moment with Surf Feature Extraction to recover attacks. Now Extracting the share 1 and it will combine with another database share 2 to generate QR-image. QR decoder will decode the Username and Password.

The beauty of our system lies in the fact that, if any attacker makes a copy of any image share to forge it later, the watermark will be distorted so for such forged image share our system will not allow the generation of host image from the stack of 2 image shares. Thus, the attacker will not get the original image.

Here we use Singular Value Decomposition discrete wavelet transform based watermarking technique which is geometrically invariant. This type watermarking scheme is robust against the RST attacks, various JPEG and noise attacks.

4. RESULTS AND ANALYSIS

4.1 Results

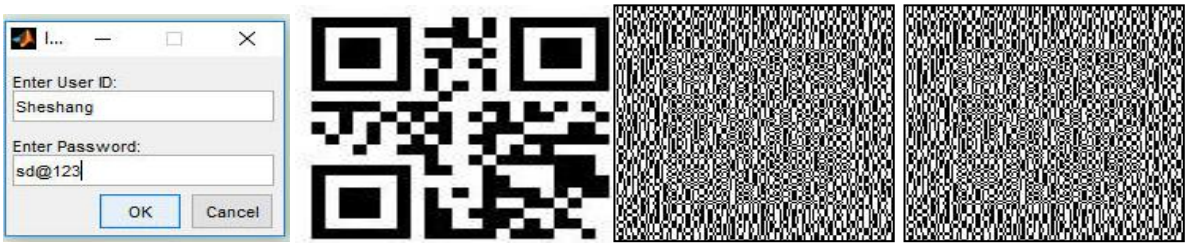

Fig 6 : (A) Enter USR and PSW **Fig 6: (B) QR-code** **Fig 6: (C) Share-1** **Fig 6: (D) Share-2**

Fig 6 : (E) Cover image **Fig 6 : (F) DWT-SVD** **Fig 6 : (G) Rotation-Scale** **Fig 6 : (H) Rotation-Tran.** **Fig 6 : (I) Scale-Tran.**

Fig 6 : (J) Recover Attack **Fig 6 : (K) Recover Image** **Fig 6 : (L) Recovered share-2** **Fig 6 : (M)) Recovered QR-code**

4.2 Analysis

Table 1: Rotation with Scale

Rotation	*Scale*	*PSNR*	*MSE*
30	2	66.063	0.023
45		64.063	0.025
102		65.023	0.019
90		66.021	0.022
120		64.011	0.024

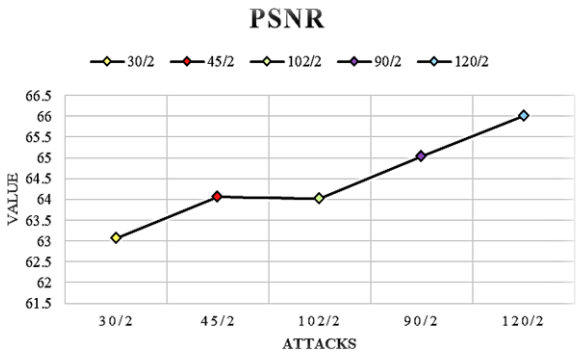

Fig 7: (A) Rotation with Scale PSNR

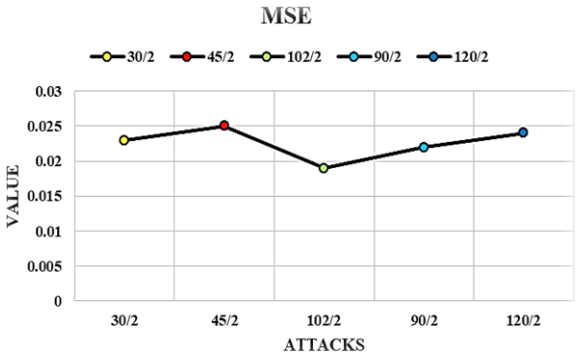

Fig 7: (B) Rotation with Scale MSE

Table 2: Rotation with Translation

Rotation	*Translation*	*PSNR*	*MSE*
30	10	66.063	0.023
45		64.063	0.025
102		65.023	0.019
90		66.021	0.022
120		64.011	0.024

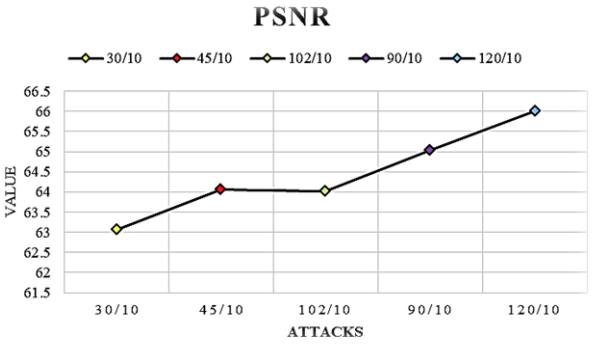

Fig 8: (A) Rotation with Translation PSNR

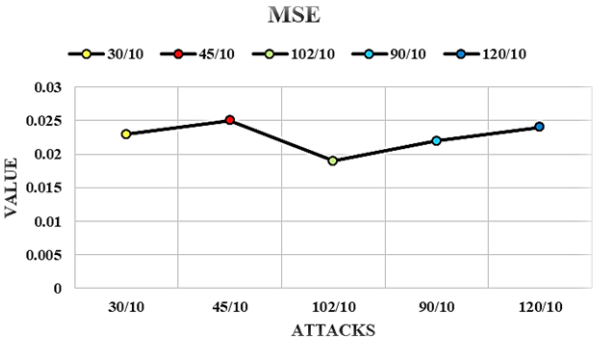

Fig 8: (B) Rotation with Translation MSE

Table 3: Translation and Scale

Translation	*Scale*	*PSNR*	*MSE*
5	2	66.063	0.023
10		64.063	0.025
-5		65.023	0.019
-10		66.021	0.022

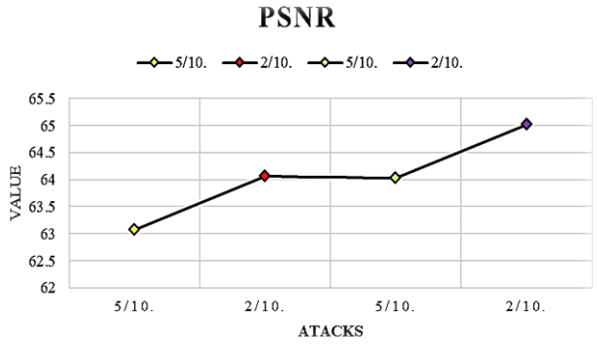

Fig 9: (A) Translation and Scale PSNR

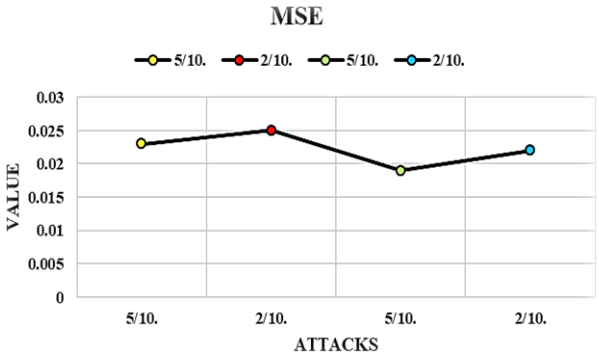

Fig 9: (B) Translation and Scale MSE

5. CONCLUSION

Proposed System has convert character into QR-code and protects against combine RST attacks on Color Cover image. For Recovery of Attacks here we have use R-component with Combine approach of Block DWT-SVD and Pseudo Zernike Moment with surf feature. Affine transformation is also apply for recover attack watermark image. So after extraction the proposed system will increase PSNR value for Recovered Image. In Future Our System Will Provide Efficient as well as Privacy Preserving Communication in Traditional Systems.

6. REFERENCES

[1] Delphin Raj K. M and Nancy Victor "Secure QR Coding of Images Using the Techniques of Encoding and Encryption" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 12 (2014) pp. 2009-2017

[2] Ajish S And Rajasree R "Secure Mail Using Visual Cryptography (Smvc)" 5th Icccnt 2014 July 11- 13, 2014, Hefei, China

[3] Akshya Kumar Gupta And Mehul S Raval "A Robust And Secure Watermarking Scheme Based On Singular Values Replacement" SaDhana Vol. 37, Part 4, August 2012, Pp. 425–440.Indian Academy Of Sciences

[4] Ali Benoraira, Khier Benma hammed And Noureddine Boucenna "Blind Image Watermarking Technique Based On Differential Embedding In Dwt And Dct Domains" Springer 2015

[5] Angelina Espejel-Trujillo, Mariko Nakano-Miyatake, And Hector Perez-Meana "New Condition For Hierarchical Secret Image Sharing Scheme" 2014 Ieee 28th International Conference On Advanced Information Networking And Applications

[6] Aparna J R And Sonal Ayyappan "Comparison Of Digital Watermarking Techniques" International Conference For Convergence Of Technology - 2014

[7] Bharat Singh, Dr. V.S. Dhaka And Ravi Saharan "Blind Detection Attack Resistant Image Watermarking" Ieee 2014

[8] Carlo Blundo, Alfredo De Santis, Moni Naor "Visual Cryptography For Grey Level Images" Information Processing Letters 75 (2000) 255–259 Elsevier

[9] Chun-Hsiang Huang And Ja-Ling Wu "Attacking Visible Watermarking Schemes" Ieee Transactions On Multimedia, Vol. 6, No. 1, February 2004

[10] Dao-Shun Wang, Member, Ieee, Tao Song, Lin Dong, And Ching-Nung Yang "Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing" Ieee Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013

[11] Deepa A K1 And Bento Benziger "Embedded Extended Visual Cryptography Scheme For Color Image Using Abc Algorithm" IEEE,Icsp 2014

[12] Dong Zheng, Yan Liu, And Jiying Zhao "A Survey Of Rst Invariant Image Watermarking Algorithms" IeeeCcece/Ccgei, Ottawa, May 2006

[13] Dr.M.A.Dorai rangaswamy And B.Padhmavathi "An Effective Blind Watermarking Scheme For Protecting Rightful Ownership Of Digital Images" Ieee 2009

[14] Farzin Ahammed T And M.K Sulaiman "A Master Share (2, N) Xor Based Visual Cryptography Scheme By Random Grids" 2015 International Conference On Control, Communication & Computing India (Iccc) , 19-21 November 2015 ,Trivandrum

[15] Hailiang Shi, Nan Wang, Zihui Wen, Yue Wang, Huiping Zhao, Yanmin Yang "An Rst Invariant Image Watermarking Scheme Using Dwt-Svd" Ieee 2012

[16] Kai-Hui Lee And Pei-Ling Chiu "Image Size Invariant Visual Cryptography For General Access Structures Subject To Display Quality Constraints" Ieee Transactions On Image Processing, Vol. 22, No. 10, October 2013

[17] Keta Raval And Sameena Zafar "Digital Watermarking With Copyright Authentication For Image Communication" 2013 International Conference On Intelligent Systems And Signal Processing (Issp)

[18] Lin Gao, Tiegang Gao, Guorui Sheng, And Shun Zhang "Robust Medical Image Watermarking Scheme With Rotation Correction" Springer 2014

[19] M. Sukumar Reddy And S. Murali Mohan "Visual Cryptography Scheme For Secret Image Retrieval" Ijcsns International Journal Of Computer Science And Network Security, Vol.14 No.6, June 2014

[20] Md. Maklachur Rahman "A Dwt, Dct And Svd Based Watermarking Technique To Protect The Image Piracy" International Journal Of Managing Public Sector Information And Communication Technologies (Ijmpict) Vol. 4, No. 2, June 2013

[21] Munesh Chandra, Shikha Pandel And Rama Chaudharl "Digital Watermarking Technique For Protecting Digital Images" Ieee 2010

[22] Pallavi Vijay Chavan ,Dr. Mohammad Atique And Dr. Latesh Malik "Signature Based Authentication Using Contrast Enhanced Hierarchical Visual Cryptography" 2014 Ieee Students' Conference On Electrical, Electronics And Computer Science

[23] Ray Smith. Hybrid Page Layout Analysis via Tab-Stop Detection. Proceedings of the 10th international conference on document analysis and recognition. 2009.Was

[24] Shyong Jian Shyu And Ming Chiang Chen "Minimizing Pixel Expansion In Visual Cryptographic Scheme For General Access Structures" 2015 Ieee.

[25] Sy C. Nguyen, Kha H. Ha And Hoang M. Nguyen "An Improved Image Watermarking Scheme Using Selective Curvelet Scales" 2015 International Conference On Advanced Technologies For Communications (Atc)

[26] Vikas Saxena "Collusion Attack Resistant Watermarking Scheme For Images Using Dct" Ieee 2014

[27] Xiaotian Wu And Wei Sun "Extended Capabilities For Xor-Based Visual Cryptography" Ieee Transactions On Information Forensics And Security, Vol. 9, No. 10, October 2014

[28] Xiao-Yi Liu, Ming-Song Chen, And Ya-Li Zhang "A New Color Visual Cryptography Scheme With Perfect Contrast" 2013 8th International Conference On Communications And Networking In China (Chinacom)

[29] Young-Chang Hou "Visual Cryptography For Color Images" IEEE Pattern Recognition 36 (2003) 1619 – 1629

[30] Herbert Bay, Andreas Ess, Tinne Tuytelaars, Luc Van Gool," Speeded-Up Robust Features (SURF)", 2007, Elsevier

[31] Sheshang D. Degadwala & Dr. Sanjay Gaur "Privacy Preserving System Using Pseudo Zernike Moment with SURF & Affine Transformation on RST Attacks" Vol. 15 No. 4 April 2017 International Journal of Computer Science and Information Security.