An Efficient Privacy Preserving System Based on RST Attacks on Color Image

Sheshang D. Degadwala(✉) and Sanjay Gaur

Madhav University, Sirohi, Rajasthan, India
sheshang13@gmail.com, sanjay.since@gmail.com

Abstract. In Development of network communication need protect the transmission with fast Communication. Therefore, networking producers need to be constantly manage illegal use of the data. In our proposed approach, first step enter the user name and password then generate in text format that will be converted to QR-code using zxing library. Now the QR-code will be converted in to the share using Binary Visual cryptography algorithm. After that generated share-2 is save in the database that is for future reference at receiver side and share-1 is embedding into the R-Component LL bit using of block DWT-SVD and Pseudo Zernike moment. In embedded image further add G, B Component. So, Color watermark image is ready to transfer from the network. As in network there are different attackers apply RST attacks on the color watermark image and Generated attack Watermark Image. At the receiver side recover the attacks first apply Pseudo Zernike moment, Surf feature on R-component so, 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 authentication to all online Services.

Keywords: QR codes · VCS · RGB-extract · Block-DWT · Surf · Affine RST attacks

1 Introduction

In the world of communication, security assumes a basic part and claims a major management looking into its data. The announcement communication not withstanding a time's doesn't venture out alone, it will be attached unit with security parts. Subsequently security turns with make the way with open a correspondence box. Approaching data security, which is spread under cryptography, majority of the data hide or loss. Furthermore watermarking gives better part concerning with the handing sensitive data. Current Systems with the preventing methods continues evolving its face for boosted features, there may be need with get updated to it for its long run towards the improvement of future. Typically those happening is that the point when another calculation is transformed alternately an existing calculation is revised, intruders alternately hackers break the calculation. Along these lines it will be an absolute necessity on create

Z. Patel and S. Gupta (Eds.): ICFITT 2017, LNICST 220, pp. 17–27, 2018.
https://doi.org/10.1007/978-3-319-73712-6_2

calculations that's only the tip of the iceberg proficient and make stable and unbreakable on the greater part degree. Normally, the organize security may be spread under cryptography and data concealing. Majority of the data concealing holds Steganography and watermarking which might be dated again old contrasted with cryptography. Done cryptography, scramble of data's takes put at those transmitter. Furthermore unscrambling them provides for those accurate enter toward those recipient area. Subsequently for scrambling Also unscrambling indicated actually Likewise encryption Furthermore decryption, a fact that utilized. Accordingly will scramble What's more unscramble same enter or distinctive keys might be utilized. Further extending its limbs under symmetric (conventional) Also deviated (public key) encryption. Here in the previous encryption, same fact that utilized both In those transmitter Also collector. Bit in the latter case, diverse fact that took care of. Advancing to Steganography, which will be craftsmanship of hiding of information under other. It might make dated past, yet once more heads should additional secure transmission. In place should enhance those security level, consolidation of Different systems will be took care of. One such attempt may be those Steganography again cryptography [2, 3].

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 (Fig. 1).

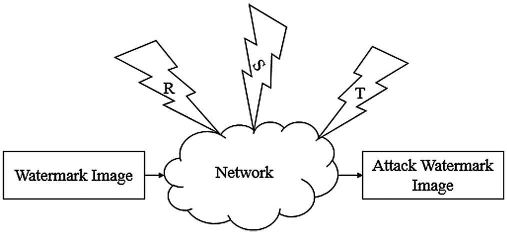


Fig. 1. Rotation (R), Scale (S) and Translation (T) attacks in network

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 cosine transform (DCT), the discrete Fourier transform (DFT) and discrete wavelet transform (DWT). Capacity of DWT-SVD based plan is more than DFT.

A wide assortment of picture watermarking plans has been proposed and every locations a wide range of use situations.

2 Literature Survey

2.1 QR-Code [1, 4]

In computer networks development, distribution of “multimedia products is becoming gradually more day to day and the problems of digital copyright have become more and more famous. However, digital watermark is the new technology in the field of copyright protection. But it cannot effectively solve the problem of the arithmetical attacks in terms of image and the impact on the QR code fast responsive” characteristics [1].

Quick Response code is “2-dimension (2D) barcode, Denso Wave Corporation developed QR code in 1994. It can be improve the reading speed of 2D-barcodes and contains data for both vertical and horizontal dimensions and that’s why it can contain a significantly greater amount of information. QD code contains information like text, web link, number, and multimedia data and is speed is 20 times faster than that of other 2D symbols. When secrete message embed into QR code, first it encode and then after develop the structure of QR code but it is time consuming, risky, and from QR code cannot get the secret message” directly [4].

2.2 VCS [2]

VCS is a new kind of cryptographic idea that efforts on resolving the problems of distribution the private images. VCS having the capacity to conceal information/data, for example, individual subtle elements is exceptionally fortunate. At the point when the information is covered up inside isolated pictures, it is altogether unrecognizable. At the point when the shares are partitioned, the information is totally ambiguous. Every picture holds distinctive bits of the information and when they are stacked together, the mystery message can be recuperated effortlessly. Every share relies on upon each other with a specific end goal to get the decoded data [2].

A pixel is a littlest component of an advanced picture. In a 32-bit advanced picture every pixel comprises of 32 bits, which is isolated into four sections, in particular red, green, blue and alpha; each with 8 bits. Alpha part introduces level of straightforwardness. In the event that each bits of Alpha part are ‘0’, then the picture is absolutely straightforward. Human visual framework goes about as an OR work. In the event that two straightforward items are stacked together, then the last heap of articles will be straightforward. Be that as it may, in the event that one of them is non-straightforward, then the last pile of items will be non-transparent. Like 0 OR 0 = 0, considering 0 as straightforward and, 0 OR 1 = 1, 1 OR 0 = 1, 1 OR 1 = 1, in view of 1 as non-straightforward.

2.3 Digital Watermarking [5]

Digital watermark is “new approach to complement cryptographic processes. It is a visible or invisible identification code that is permanently embedded in the data and remains present within the data after any decryption process [7]. The idea of computerized watermarking is gotten from steganography. Both steganography and watermarking plans are utilized to exchange data by implanting it into the" cover pictures [6].

A wide assortment of picture watermarking plans has been proposed and every locations a wide range of use situations. 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 ordered into the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) and so forth. Vigor is great in DWT based plan than DFT [5].

3 Proposed Preserving 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.

QR-Generation: As shown in the Fig. 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.

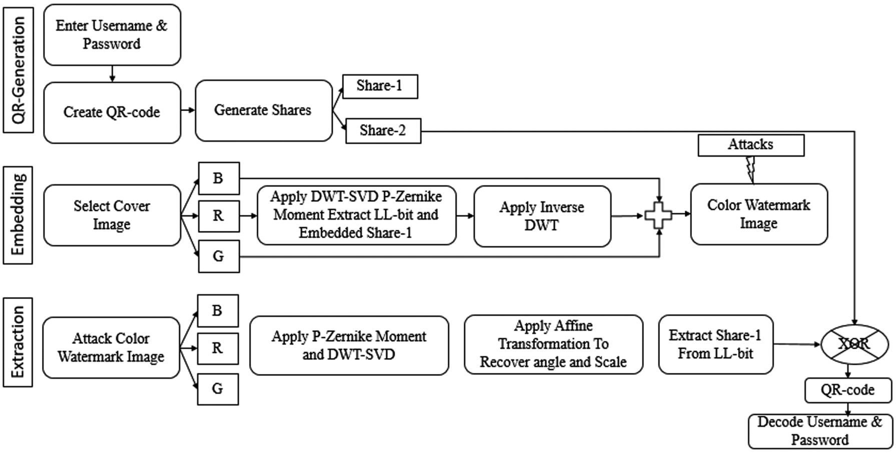

QR-Generation
Enter Username & Password
Create QR-code
Generate Shares
Share-1
Share-2
Embedding
Select Cover Image
B
R
G
Apply DWT-SVD P-Zernike Moment Extract LL-bit and Embedded Share-1
Apply Inverse DWT
Attacks
Color Watermark Image
Extraction
Attack Color Watermark Image
B
R
G
Apply P-Zernike Moment and DWT-SVD
Apply Affine Transformation To Recover angle and Scale
Extract Share-1 From LL-bit
XOR
QR-code
Decode Username & Password

Fig. 2. Proposed flow

Embedding: In this process as shown in the Fig. 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.

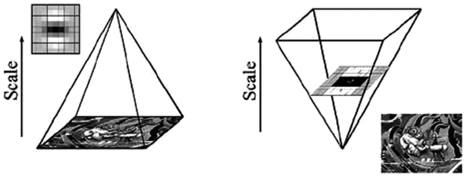


Fig. 3. Surf feature

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.

3.1 Overall System

3.1.1 Encoder

Step 1: Enter User name and Password
Step 2: Encode to QR-Image
Step 3: Apply VCS and Generate 2-Share
Step 4: Share 2 is Save in Database
Step 5: Select Color Cover Image
Step 6: Extract R-Component
Step 7: Apply Block DWT + SVD + Pseudo Zernike Moment
Step 8: Embedding Share 1 in LL-band, G and B to Generate Watermark image

3.1.2 Network

Apply Rotation, Scale and Translation on Watermark Image.

3.1.3 Decoder

Step 1: Read Attack Watermark Image
Step 2: Extract R-Component
Step 3: Apply Pseudo Zernike Moment
Step 4: Apply Surf Feature Extraction and Affine Transformation
Step 5: Recover Rotation, Scale and translation Attacks
Step 6: Apply Block DWT + SVD
Step 7: Extract Share1 from LL-band
Step 8: Combine Share 1 and Share 2
Step 9: Decode QR-Image
Step 10: Recover User name and Password

3.2 VCS Algorithm

3.2.1 Share Generation

Generating those stakes from claiming mystery Image: in this stage usage from claiming Visual cryptography [2] may be completed. It includes those making of stakes starting with mystery picture utilizing (2, 2) VCS plan. Precise principal the mystery picture will be taken What's more is changed over should a double picture that point each pixel in the mystery picture is partitioned under eight sub pixels, four pixels in every impart Toward selecting the irregular pixel encoding plan crazy about scheme provided in algorithm.

3.2.2 Share Combination

In the keep going phase, those methodology for VCS mix may be performed. Here toward applying those double XOR operation, on both shares, we will get original data.

3.2.3 Embedding Algorithm

Step 1: Encode QR-image of Username and Password using Zxing 1.6 Library of java.

Step 2: Give Y a chance to signify the watermark inserting part, and utilize Haar orthogonal wavelet Transform to Y; then pick up the band LL which has most extreme vitality. Distribute LL into blocks Bi of size 4 × 4,

$$\mathrm{Z}'' = [\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3 \ldots\ldots, \mathrm{a}_\mathrm{s}]$$

Where Zj″ is vector, and a_i is the SVD of all block, S is rank of all block.

Step 3: Apply the straightforward strategic monitor on encrypt the watermark.

$$x_{n+1} = \mu x_n \left(1 - x_n\right), 0 < x_n < 1, n = 0, 1, 2 \ldots..10$$

Step 4: Calculate the value of Zj″

Norms Zj″ = $\sqrt{\sum_{\mathrm{j}=1}^{\mathrm{s}} \mathrm{a}_\mathrm{j} * \mathrm{a}_\mathrm{j}}$ and then NO″ = Norms (Zj″)/D.

Step 5: Embed bit using following technique.
If b = 1 then {if O is odd then O′ = O +1 else O′ = O} {Else {if E is even then E′ = E else E′ = E +1}}.

Step 6: Calculate the modified value and the modified vector as follows:

$$\mathrm{Norms}\left(\mathrm{Zj}'\right) = \mathrm{NO}' \times \mathrm{D} + (\mathrm{D}/2),\ \mathrm{Zj}' = \mathrm{Zj} \times \mathrm{Norms}\ (\mathrm{Zj}')/\mathrm{Norms}\ (\mathrm{Zj})$$

Step 7: Apply inverse DWT to generate watermarked image.

3.2.4 Recover Decoding Algorithm

Step 1: To gauge the utilization of ensured Pseudo Zernike moments

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

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

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

A = absolute (Z)
Angle (Z) = tan − 1(imag(Z), real(Z));
Phi = angle (Z) * 180/pie

Step 2: Surf Feature exact [8]

Sense importance points, use Hessian matrix estimation. Form the integral pictures and the scale space of picture.

Importance point explanation and equivalent, descriptor defines the circulation of the intensity content, alike to SIFT. Based on sum of Haar wavelet reactions, construct a square region centered everywhere the interest point and concerned with along the location selected in earlier slice.

Step 3: pick up the Recovered watermarked image, and actualize 1-level DWT disintegration to its watermark embedding part. Get the sub-band LL′ which has incomparable vitality.

Step 4: Slice the sub-band LL″ into blocks Bi of size 4 × 4,

$$\mathrm{Zj}'' = [\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3 \ldots \ldots, \mathrm{a}_\mathrm{s}]$$

Where Zj″ is a vector, and a_i is the SVD of all block and S is rank of all block.

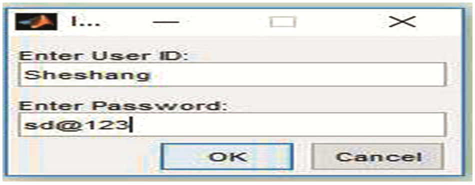
Step 5: Calculate the value of Zj″,

Norms Zj″ $= \sqrt{\sum_{\mathrm{j}=1}^{\mathrm{s}} \mathrm{a}_\mathrm{j} * \mathrm{a}_\mathrm{j}}$ and the NO″ = Norms(Zj″)/D.

Step 6: Extract bit and extract watermark.
Step 7: Stacked extracted image with database share image with XORed operation.
Step 8: Decode QR-image to recover Username and Password.

4 Results and Discussion

As shown in Fig. 4 First user have to enter user name will enter by the user and Fig. 5 will be the QR-code generated by zxing library. Figure 6 is share 1 image generated by apply VCS algorithm.


I...

Enter User ID:
Sheshang

Enter Password:
sd@123

Fig. 4. ID & PSW

Fig. 5. QR-code

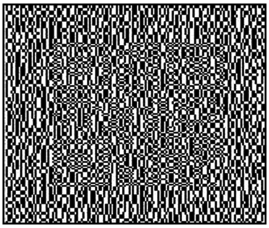


Fig. 6. Share 1

As shown in Fig. 7 Color image the DWT-SVD to getting the LL-bit as shown in Fig. 8. This image is now Combine with G and B to Create Color Watermark image. Attacker apply Rotation Attacks so getting the Fig. 9 image with rotation angle 30° (Table 1).

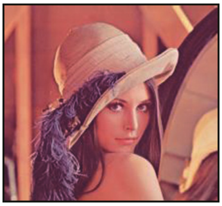


Fig. 7. Cover image

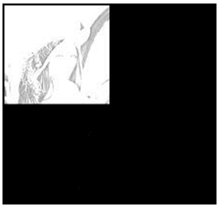


Fig. 8. DWT LL bit

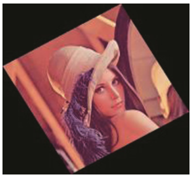
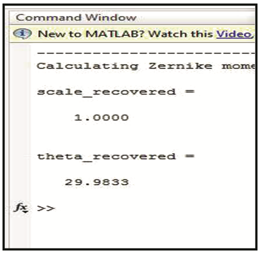


Fig. 9. Rotation 30°

Table 1. Results discuss

Rotation (Degree)	30°	45°	75°	90°	180°	270°
PSNR	63.21	63.13	63.03	Inf	Inf	Inf
MSE	0.026	0.026	0.025	0	0	0
Scaling	2	3	4	5		
PSNR	Inf	Inf	Inf	Inf		
MSE	0	0	0	0		
Translation	−10	−20	10	20		
PSNR	73.72	72.44	Inf	72.27		
MSE	0.0033	0.0055	0	0.0695		

Figure 10 shows the recover angle and Scale. Figure 11 will be generated by the P-pseudo Zernike and Surf Transformation. Figure 12 is Recover Share 1 from RST attacks. Figure 13 be the Recover the Username and password by decoding QR (Figs. 14 and 15).



```
------------------------
Calculating Zernike mome
scale_recovered =

    1.0000


theta_recovered =

   29.9833

fx >>
```

Fig. 10. Recover data

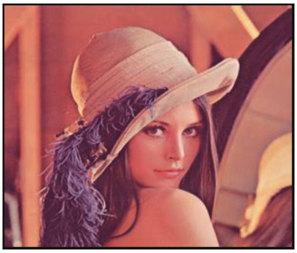


Fig. 11. Recover image

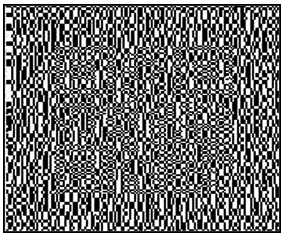
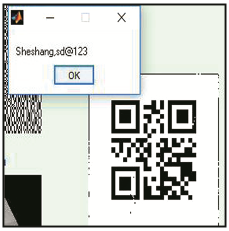


Fig. 12. Share 1



Sheshang,sd@123

Fig. 13. Recover UID & password

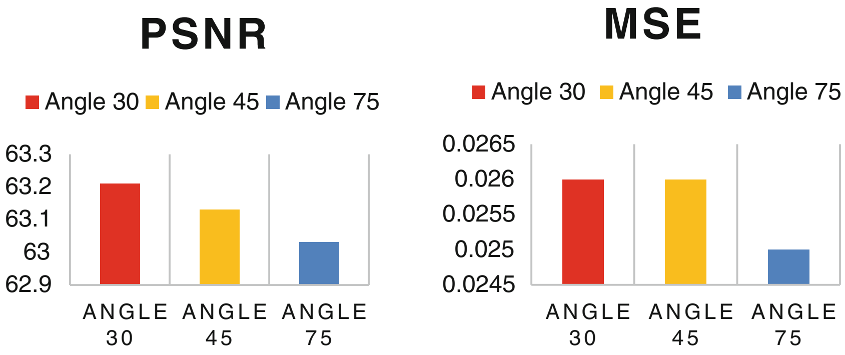


Fig. 14. Graphical representation of PSNR and MSE of Rotation Attacks

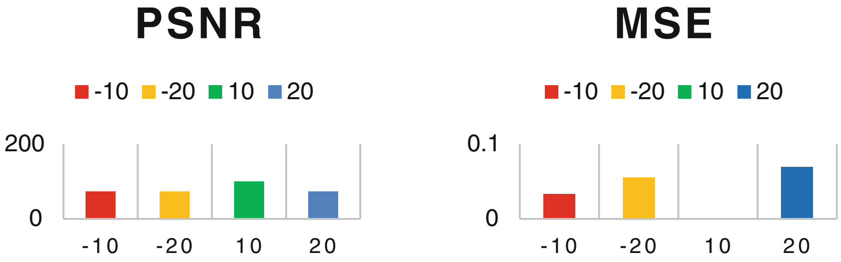


Fig. 15. Graphical representation of PSNR and MSE of translation attacks

5 Conclusion

In our proposed System we have convert username and password into QR-code. The QR-code is further divided into shares that shares are embedding into cover image. So its call multilayer Privacy. Now whenever Dual RST attacks apply on Color Cover image between transmission and receiving. Our Privacy Preserving System Recover Attacks. Here we have use Block DWT-SVD and Pseudo Zernike Moment with surf feature based watermarking system. Affine transformation is also apply for recover attacks on watermark image. So after extraction the proposed system will increase PSNR value for Recovered Image. This System Will Provide Efficient as well as Privacy Preserving Communication in Traditional Systems.

References

1. Delphin Raj, K.M., Victor, N.: Secure QR coding of images using the techniques of encoding and encryption. Int. J. Appl. Eng. Res. **9**(12), 2009–2017 (2014). ISSN 0973-4562
2. Ajish, S., Rajasree, R.: Secure mail using visual cryptography (SMVC). In: 5th ICCCNT 2014, 11–13 July 2014, Hefei, China (2014)
3. Gupta, A.K., Raval, M.S.: A robust and secure watermarking scheme based on singular values replacement. SaDhana **37**(4), 425–440 (2012)

4. Benoraira, A., Benmahammed, K., Boucenna, N.: Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP J. Adv. Sig. Process. **2015**, 55 (2015)
5. Gao, L., Gao, T., Sheng, G., Zhang, S.: Robust medical image watermarking scheme with rotation correction. In: Pan, J.-S., Snasel, V., Corchado, E.S., Abraham, A., Wang, S.-L. (eds.) Intelligent Data analysis and its Applications, Volume II. AISC, vol. 298, pp. 283–292. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07773-4_28
6. Nguyen, S.C., Ha, K.H., Nguyen, H.M.: An improved image watermarking scheme using selective curvelet scales. In: 2015 International Conference on Advanced Technologies for Communications (ATC) (2015)
7. Saxena, V.: Collusion attack resistant watermarking scheme for images using DCT. IEEE (2014)
8. Bay, H., Ess, A., Tuytelaars, T., Van Gool, L.: Speeded-up robust features (SURF). Comput. Vis. Image Underst. **110**, 346–359 (2007)