CSVTU International Journal of Biotechnology, Bioinformatics and Biomedical
Vol. 4(2), 59–66, 2019 ISSN: 2455-5762

Research Article

Virtual Cryptopgraphic Technique and Bit-plane Segmentation Stegnegography for Security in Bioinformatics and Biomedical Applications

Dr Tin Mar Kyi[1] and Abhishek Misal[2]

[1]Professor, Myanmar Institute of Information Technology Mandalay Myanmar
[2]Chhattisgarh Swami Vivekanand Technical University, Bhilai India 491107
tin_mar_kyi@miit.edu.mm[1], abhishekmisal18@gmail.com[2]

Received August 16, 2019; received in revised form August 27 2019; accepted August 28, 2019; Available online August 2019

Abstract

The security techniques are very important in all modern bioinformatics applications since most of the applications of biomedical science and engineering are using digital media and processing. There are several security techniques for protection of various types of data, such as biometrics, cryptograpy, watermarking etc. This paper discusses about cryptographic methods only and virtual cryptopgraphy has been implemented successfully with considerable improvement in signal quality. The importance of the virtual cryptography is emphasized that can be used to protect and secure various types of data involved in bioinformatics and biomedical applications. The bit-plane segmentation stagenography enhances the security and also helps in better protection of data.

Keywords: Security, cryptography, data, bioinformatics, biomedical application.

1. Introduction

Recently, internet has become increasingly popular and used in several applications all over the world. Nowadays, internet banking system has become increasingly popular and is widely used in currency. The system of visual cryptography is implemented to secure data which is bioinformatics data that may be data related to protein synthesis, DNA analysis, EEG analysis and communication etc. [1-5]. Security text is used as the user input which is converted into an image by using captcha image generation process [6-9]. The captcha image is split into share1 and share2 based on the visual cryptography. The share2 is hidden into the uploaded cover image by using general purpose steganography and sends it into user's email account and user must download it. The share1 is kept at server database and during login process, user logs in with the stego image. The share2 is extracted from stego image using steganography. Both share1 and share2 are stacked by using visual cryptography to reveal the captcha image, and then one-time password is sent to user's mobile. The main objectives of the work related to cryptography for bioinformatics and biomedical applications are:

- To present overview and implement the visual cryptography sharing scheme and bit-plane complexity segmentation steganography
- To provide better security

Visual cryptography is initially limited for gray scale images which employ a basically a threshold scheme where secret image is given to two shares. Original data is decided into two shares in (2.2) scheme [8-14]. The scheme operates in following ways:

i. Input image or data is read

ii. Random binary image is created

iii. XOR operation is performed on share 1 and the result is share 2 data

iv. Each pixel is separated on the basis of either 2 sub-pixels or 4-sub pixels' information.

This can be seen in Fig. 1.

Original Pixel	Share 1	Share 2	Share1 + share 2	Result (XOR)
□ 0	□■ 0 1	□■ 0 1	□■ 0 1	□ 0
	■□ 1 0	■□ 1 0	■□ 1 0	□ 0
■ 1	■□ 1 0	□■ 0 1	■■ 1 1	■ 1
	□■ 0 1	■□ 1 0	■■ 1 1	■ 1

Figure 1 Visual cryptography scheme.

An example of operation is shown in Fig. 2.

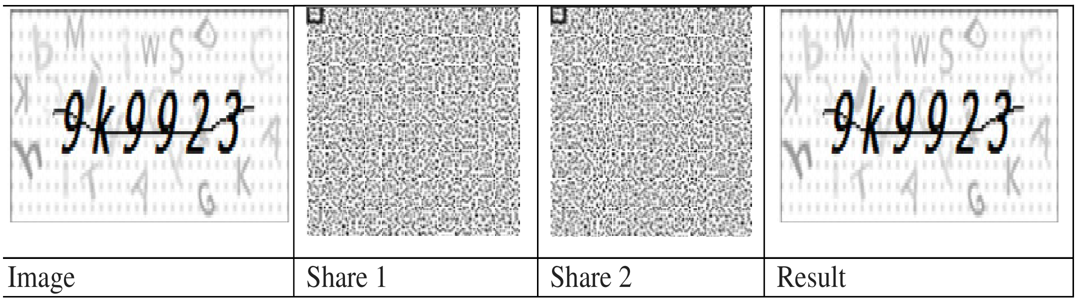

Figure 2 Sample result of Visual cryptography scheme

There are several methods for cryptography for various data like protein structure, highlighted and discussed [1-3, 10-14] but especially for bioinformatics data and biomedical data, due to their specific properties, methods were not implemented particularly.

1. 1 Proposed Method

A system is constructed with registration and login processes which is implemented with the combination of steganography and visual cryptography. In the registration process, the user registers his/her personal information which is used as input. Then this input is converted into an image by using captcha image generation process. This captcha image is splitted into share1 and share2 based on the visual cryptography. The share2 is hidden into the uploaded cover image by using BPCS steganography and sends it into user's email account and user must download it.

In login process, user enters with four steps to this internet banking. The user must enter two characters of the secret text in the first step. Secondly, user browses stego image. The user needs to type the text displayed in the captcha image in the third step. The user login the system with one-time password by using Telerivet mobile Messaging in the final step.

This captcha image is split into share1 and share2 based on the visual cryptography are shown in Fig. 3, Fig. 4 and Fig. 5. After uploading a cover photo, share2 (user's share) is hidden in this cover image by using BPCS algorithm. Then this image is sent to user's email account and user must download it. The system's administrator stores the share1 into the database for checking the user in login process. The user needs to save this stego-image because user must log in with this stego-image.

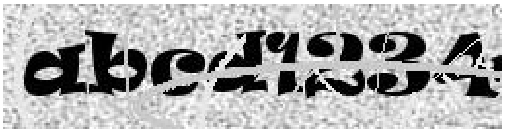

Figure 3 Captcha Image

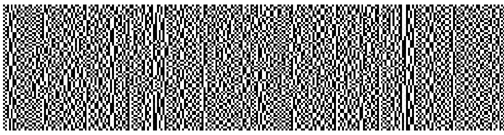

Figure 4 Share1

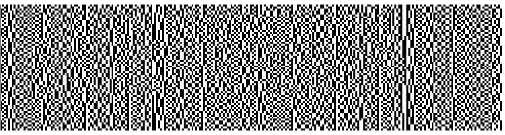

Figure 5 Share2

Firstly, user enters username, account number and first two characters of the secret text. Secondly, user browses stego-image in order to extract share2 from it. The stego-image and the extracted share2 image are shown in Fig. 6 and Fig. 7. In the third step, the extracted share2 and the share1 are superimposed by using visual cryptography. If the security text is checked with that the user has entered at the time of registration, the captcha image is displayed. The captcha image is shown in Fig. 8. The user needs to type the text displayed in the captcha image. The one-time password (OTP) is sent to user's mobile by using Telerivet Mobile Messaging. The user uses this OTP as the password in the final step. It is described in Fig. 9. If the user is accepted for online banking, the user reaches the system home page. He/she can deposit money, withdraw money and know his/her balance. This system is implemented by using PHP Programming Language.

Figure 6 Stego-image

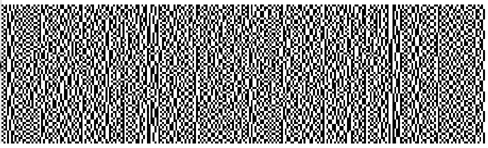

Figure 7 Decrypted Share2

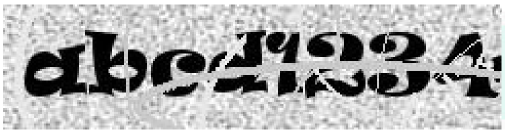

Figure 8 Captcha Image

Figure 9 One-time Password

The performance of cryptograpy and stegenography was evaluated in terms of performance metrics, such as mean absolute error (MAE), number of pixels change rate (NPCR), maximum difference (MD), normalized absolute error (NAE), MSE and PSNR, mean opinion score (MOS).

2. Results and Discussion

This system is tested with fourteen image sizes (pixels) with three different formats of image (PNG, BMP, JPEG) are tested with NPCR, PSNR, MSE and MOS. This system is tested between original cover image and secret image (stego-image).

Table 1 NPCR values for PNG Images

Image Size (pixel)	NPCR (%)
424×104	76.01
432×112	70.29
440×120	66.16
448×128	60.93
456×136	56.82
464×144	53.33
472×152	50.18
480×160	46.18
488×168	42.86
496×176	40.82
504×184	39.41
512×192	36.98
520×200	36.38
528×208	34.08

The fourteen image pixels are 424×104, 432×112, 440×120, 448×128, 456×136, 464×144, 472×152, 480×160, 488×168, 496×176, 504×184, 512×192, 520×200 and 528×208. NPCR and UACI values of PNG image formats with fourteen image sizes are shown in Table 1. NPCR values of BMP and JPEG image formats are shown in Table 2 and Table 3.

Table 2 NPCR values for BMP Images

Image Size (Pixel)	NPCR (%)
424×104	75.96
432×112	70.51
440×120	66.31
448×128	61.07
456×136	56.57
464×144	53.50
472×152	50.29
480×160	46.12
488×168	42.91
496×176	41.08
504×184	39.36
512×192	36.96
520×200	36.38
528×208	34.22

The pixel size of the images is less then NPCR values are high. The image pixel size 424×104 is the highest NPCR value and 528×208 image pixel size is the lowest values of NPCR. The value of NPCR in the system indicates that the less value of the image pixel size is, the better the security level. The image quality between cover image and stego-image is measured by using PSNR and MSE methods. The values of PSNR and MSE in fourteen images sizes with three image formats (PNG, BMP, and JPEG) were obtained but values are shown in Table 4 for PNG images here.

Table 3 NPCR values for JPEG Images

Image Size (Pixel)	NPCR (%)
424×104	75.84
432×112	70.66
440×120	66.39
448×128	60.78
456×136	56.61
464×144	53.50
472×152	50.18
480×160	46.18
488×168	41.93
496×176	40.97
504×184	39.45
512×192	36.93
520×200	36.34
528×208	34.25

After testing, PSNR values of 528×208 image size are larger than other image sizes and MSE values of 528×208image size are smaller than other image sizes. When the image size is large, the value of PSNR is large and that of MSE is small. So, the stego-image is less distortion from the original image. The visual quality between original and stego images depending on own opinion is also tested for three image formats (PNG, BMP, JPEG) with MOS. There are 10 original and stego images for testing. The image quality between original share2 and share2 extracted from stego image with adding variance noise varying from 0.0001 to 0.1is also measured by using PSNR and MSE as shown in Table 5, Table 6 and Table 7.

Table 4 PSNR and MSE values of PNG images

Image Size (Pixel)	PSNR (dB)	MSE
424×104	29.93	33.40
432×112	25.58	34.09
440×120	22.61	34.62
448×128	20.80	34.98
456×136	18.78	35.43
464×144	16.55	35.98
472×152	15.60	36.23
480×160	15.19	36.35
488×168	14.67	37.23
496×176	12.07	37.35
504×184	10.98	37.76
512×192	10.13	38.11
520×200	8.34	38.96
528×208	7.95	39.16

After testing, the image quality is not good because PSNR values are almost near 27 dB and MSE values are 110.The stego image with Gaussian noise is by using BPCS steganography. The output image (share2) is not stacked with share1. The captcha image cannot display. This system is sensitive and security level is high.

Table 5 PSNR and MSE values between original share2 and share2extracted from stego image with adding Gaussian noise with variance from 0.0001 to 0.001

Image Size	Variance = 0.0001		Variance = 0.0005		Variance = 0.001	
	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE
424×104	27.49	116.94	27.47	117.45	27.4	119.14
432×112	27.52	115.94	27.51	116.24	27.45	117.64
440×120	27.53	115.68	27.52	115.79	27.52	116.11
448×128	27.57	114.55	27.57	114.66	27.54	115.49
456×136	27.61	113.66	27.61	113.81	27.57	114.75
464×144	27.62	113.34	27.61	113.52	27.59	113.94
472×152	27.63	112.98	27.62	113.36	27.61	113.58
480×160	27.64	112.79	27.63	113.06	27.62	113.41
488×168	27.65	112.62	27.65	112.56	27.64	112.75
496×176	27.74	110.15	27.69	111.41	27.67	112.13
504×184	27.74	110.14	27.71	111.06	27.69	111.35
512×192	27.74	110.13	27.73	110.52	27.72	110.75
520×200	27.75	110.02	27.74	110.21	27.73	110.62
528×208	28.82	86.06	28.77	86.92	28.81	87.25

Table 6 PSNR and MSE values between original share2 and share2extracted from stego image with adding Gaussian noise with variance from 0.002 to 0.01

Image Size	Variance = 0.002		Variance = 0.005		Variance = 0.01	
	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE
424×104	27.41	119.27	27.39	119.29	27.39	119.53
432×112	27.4	119.21	27.39	119.27	27.39	119.41
440×120	27.42	118.73	27.42	118.79	27.41	119.03
448×128	27.48	117.15	27.47	117.33	27.42	118.73
456×136	27.49	116.63	27.49	116.77	27.45	117.92
464×144	27.55	115.29	27.54	115.57	27.48	116.95
472×152	27.59	113.95	27.59	114.07	27.53	115.86
480×160	27.61	113.52	27.61	113.79	27.58	114.29
488×168	27.64	112.92	27.61	113.69	27.63	113.23
496×176	27.66	112.35	27.65	112.58	27.64	112.77
504×184	27.68	111.78	27.68	111.92	27.66	112.22
512×192	27.69	111.45	27.68	111.79	27.68	111.91
520×200	27.71	111.08	27.71	111.22	27.68	111.73
528×208	28.75	87.46	28.61	90.24	27.73	110.47

Table 7 PSNR and MSE values between original share2 and share2extracted from stego image with adding Gaussian noise with variance from 0.02 to 0.1

Image Size	Variance = 0.02		Variance = 0.03		Variance = 0.06		Variance = 0.1	
	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE
424×104	27.39	119.64	27.38	119.84	27.38	119.91	27.34	120.98
432×112	27.39	119.55	27.38	119.77	27.38	119.89	27.35	120.75
440×120	27.39	119.42	27.39	119.52	27.38	119.77	27.36	120.27
448×128	27.41	119.05	27.39	119.37	27.39	119.54	27.37	120.05
456×136	27.43	118.43	27.42	118.67	27.4	119.24	27.38	119.88
464×144	27.47	117.27	27.45	117.98	27.44	118.12	27.42	118.67
472×152	27.49	116.84	27.47	117.24	27.45	117.91	27.43	118.49
480×160	27.52	115.96	27.52	116.02	27.46	117.49	27.46	117.72
488×168	27.56	114.87	27.55	115.15	27.51	116.29	27.46	117.52
496×176	27.64	112.87	27.61	113.55	27.58	114.34	27.54	115.46
504×184	27.67	112.05	27.67	112.17	27.63	112.98	27.62	113.41
512×192	27.67	112.01	27.67	112.07	27.66	112.27	27.64	112.77
520×200	27.64	111.91	27.67	112.01	27.67	112.13	27.66	112.41
528×208	27.73	110.55	27.73	110.64	27.72	110.77	28.09	101.54

3. Conclusions

Image steganography and visual cryptography is more and more important in today's multimedia world and biomedical images. In this system, three image formats (PNG, BMP, JPEG) with fourteen different pixel sizes are tested for measuring encryption quality and image quality. The security level of this system is tested between original image and stego-image with three image formats by using NPCR and UACI. In general, the value of both NPCR and UACI should be high for a better system. After testing, when image pixel size is less, both of the NPCR and UACI values of three image formats are large. Therefore, the better security level is in the smaller image pixel size. The image quality of the system between original image and stego-image is also measured with PSNR and MSE. This system finds that higher the PSNR value and the lower the value of MSE in the higher pixel size. So, the quality of the image is better in the higher pixel size. In average, the encryption quality of BMP image format is better than other image formats and the image quality of the stego-image is near identical to the original image. MOS score of this system is good because MOS values are almost 4 for each image of three image formats. When Gaussian noise with variance varying from 0.0001 to 0.1 is added to the stego image, the captcha image is not displayed. This system does not accept any noises. Therefore, this system is sensitive and security level is high. After testing with fourteen different pixels of cover image, cover image is not convenient with larger than 528×208 pixels for the system. So, this system is convenient for registration that the cover image is 528×208 pixel size for PNG, BMP and JPEG. This system is only used for gray cover images.

Text-based captcha is used in the login process in order to provide higher security. The text-based captcha can be extended with other captcha methods such as image-based captcha, audio-based captcha and video-based captcha.This system can also be extended by using other cryptography on several platforms.

Conflicts of interest

There are no conflicts of interest.

References

1. Sinha, G. R. 2017. Image Processing Tools for Improved Visualization and Analysis of Remotely Sensed Images for Agriculture and Forest Classifications, Agriculture and Forestry Journal, 1(1), pp. 27-32.
2. Sinha, G.R., Thakur, K. and Vyas, P., 2017. Research Impact of Astronomical Image Processing, International Journal of Luminescence and Applications, 7(3-4), pp. 503-506, October-December.
3. Kashyap, N., and Sinha G.R., 2012. Image watermarking using 2-level DWT, Advances in Computational Research, 4(1), pp.-42-45.
4. Joppe W, Bos, K. Lauter, Jake L., and Naehrig, M. 2013. Improved security for a ring-based fully homomorphic encryption scheme. In Cryptography and Coding, pages 45–64, Springer.
5. Joppe W Bos, Kristin Lauter, and Naehrig, M. 2014. Private predictive analysis on encrypted medical data. Journal of biomedical informatics, 50:234–243.
6. Brakerski, Z. 2012. Fully homomorphic encryption without modulus switching from classical GapSVP. In Reihaneh SafaviNaini and Ran Canetti, editors, CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 868–886. Springer.
7. Brakerski, Z., Gentry, C. and Halevi, S., 2013. Packed ciphertexts in lwe-based homomorphic encryption. In Public Key Cryptography–PKC 2013, pages 1–13. Springer.
8. Sinha, G.R., Thakur, K. and Kowar, M.K. Speckle reduction in Ultrasound Image processing, Journal of Acoustical. Society of India, 35(1), pp. 36-39.
9. Sinha, G.R., Thakur, K. and Kowar, M.K. (2008). Contrast Enhancement of Underwater Images, Journal of Acoustical. Society of India, 35(1), pp. 33-35.
10. Sinha, G.R. 2015. A Chapter on Fuzzy based Medical Image Processing, A volume in the Advances in Medical Technologies and Clinical Practice (AMTCP) Book Series, pp. 45-61, IGI Global Publishers, USA, IGI Global Copyright.
11. Brakerski, Z., Gentry, Craig and Vaikuntanathan, V., 2012. Fully homomorphic encryption without bootstrapping, In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, pages 309–325. ACM.
12. Brakerski, Z., 2013. Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehle, Classical hardness of learning with errors, In Proceedings of the forty-fifth annual ACM symposium on Theory of computing, pages 575–584. ACM.
13. Wang, Z. and Yu, Z., 2011.Index-based symmetric DNA encryption algorithm, Proceedings of the 4th International Congress on Image and Signal Processing, 15-17 October, Shanghai, pp.2290-2294.
14. Zhang, Y., Fu, B. and Zhang, X., 2012. DNA cryptography based on DNA fragment assembly, Proceedings of the IEEE International Conference on Information Science and Digital Content Technology, Vol. 1, 26-28 June, Jeju, pp.179-182.