Research and Development of the Encryption Algorithm in Specific Area of Digital Image with Viola and Jones Face Detection Algorithm

R. Bustami [1], I. Klimov [2]

Izhevsk State Technical University, Izhevsk, Russia
E-mail: [1] ridho.bustami@gmail.com, [2] klimov@istu.ru

Received: 23.10.2015

Abstract. Protecting our information data from third party such as data confidentiality is one aim of cryptography system. Therefore in this paper showed the technique of encryption algorithm for digital image, which encrypted specific area such as face. Simulation describes the technique of detecting, cropping, rearranging, encrypting and decrypting on detected face in image with Viola and Jones algorithm. Using two symmetric block cryptography algorithm: Data Encryption Standard and GOST 28147-89, and also image encryption based on chaotic system. Then simulation is showed in graphic user interface in Matlab.

Keywords: cryptography system, digital image, Viola and Jones algorithm, symmetric block, Data Encryption Standard, GOST 28147-89, chaotic system

INTRODUCTION

Taking photos with mobile phone and storing in the cloud system are nowadays become a common trends. Cloud system is a common used because of increasing on Internet speed and operation system mobile phone like android or I-phone. In the future, data don't need to be saved in personal drive, data automatically will be saved or processed in the cloud system.

Selfie is becoming popular trend that people take their selves photos with own mobile phone. Beside of that, the mobile phone camera also is being developed, especially for increasing pixel to make images better and sharper and also still has good quality if seen in the another media, like personal computer even for printing.

Recently famous actress have got a problem with their selfie photos, when they think I-cloud which created by Apple.inc has secure system, they saved their photos in the I-cloud which connect automatically with their mobile phone. And after third party cracked the apple system, and shared famous actress photos which contains some personal privacy. After the photos leaked, they could do nothing with that, just some kind law of punishment they could do that, but they couldn't bring back their photos.

Actually, if our mobile phone get lost or stolen, if not prepared about that happen, our data can't be secured. Indeed, mobile phone has password protecting, but it's not enough because unresponsive people still can access our data via memory card. It can't be ignored, and also have to be awarded with our data.

METHOD OF CRYPTOGRAPHY

So here introduces a method protecting our digital photo especially taken by selfie. Based on oxford dictionary selfie means “A photograph that one has taken of oneself, typically one taken with a smartphone or webcam and shared via social media”. But actually sometimes photos not to be shared via social media because some reason of privacy that users don't want to share to public.

A method that presented is encrypting only in important part of image. In selfie photos, usually the important area or part is at face or faces. In each face will be detected automatically and directly encrypted. Based on this idea, the time processing for encrypting and decrypting image will be reduced and also make privacy in image better.

One of the method for face detection is Viola-Jones algorithm. The Viola–Jones object detection framework is the first object detection framework to provide competitive object detection rates in real-time proposed in 2001 by Paul Viola and Michael Jones [1]. Algorithm for encryption that used is Data Encryption Standard DES [2, 4], GOST 28147-89 [3–4], Logistic Map-One time pad.

EXPERIMENT OF ALGORITHMS

In experiment, divided into 4 general step, First step is detecting Face with Viola–Jones object detection algorithm. Before this step digital image has to convert to value of pixel. The input is digital image which has inside at least one face. Face will be detected by Viola and Jones algorithm. Coordinates of pixel (x, y) and also length of detected part will be saved in database.

Second step is preparing selected image to encryption block if uses DES & GOST. If DES or GOST is used, value of pixel need to convert to binary data with length 64 bit and also preparing key 64 bit for DES and 256 bit for GOST. If Logistic Map-One time pad is used, the value data don't to needed convert to bit because algorithm working in decimal values.

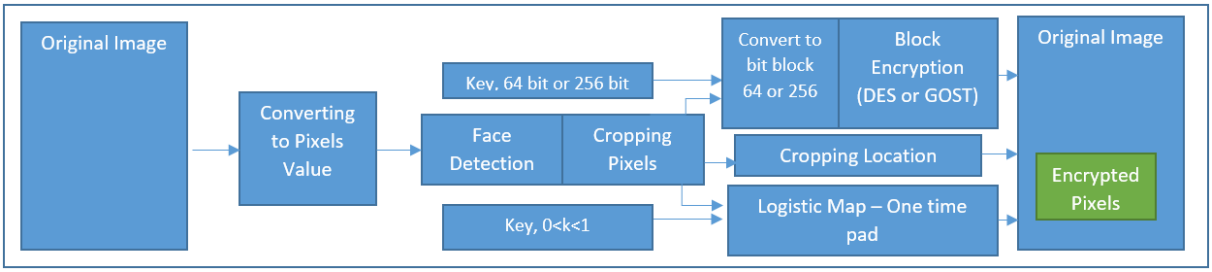

Figure 1. Schema encryption in specific area with face detection algorithm

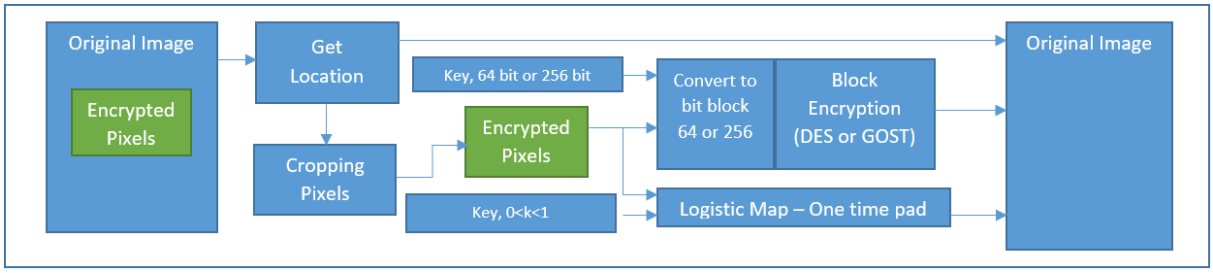

Figure 2. Schema decryption in specific area with face detection algorithm

Third Step is encryption and decryption process. Working with encryption and description is depended on cryptography algorithm that we used (DES, GOST or Logistic Map – One Time pad). In this step every algorithm works dependently each other.

Final Step is collecting from image and rearranging into image. In this step after encryption or decryption process, the pixel which already encrypted or decrypted need to be collected and rearranged into main image. Coordinates of pixel and length will be obtained from database.

SIMULATION

In this simulation, we use Matlab 2012 programming language for this design. Beside of that, created graphical user interface which make easier for people who use this simulation. At the first step just uploaded photos which one face or more is available. After that the program directly detect and encrypt. In decrypting process, actually beside the key for decrypting the system need to know information which place that already encrypted. Decrypted area will be replaced again like in encryption process.

Figure 3. Main page of simulation on Matlab using graphics user interface

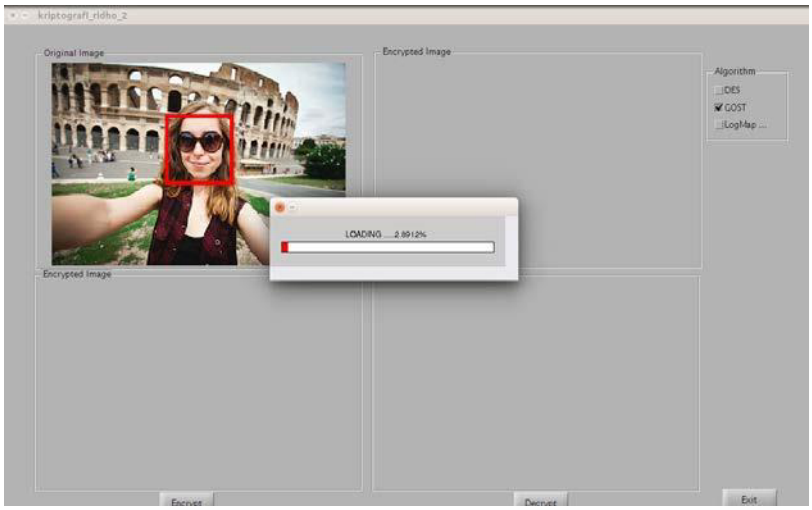

Figure 4. First step, detecting face with Viola and Jones algorithm and encrypting process

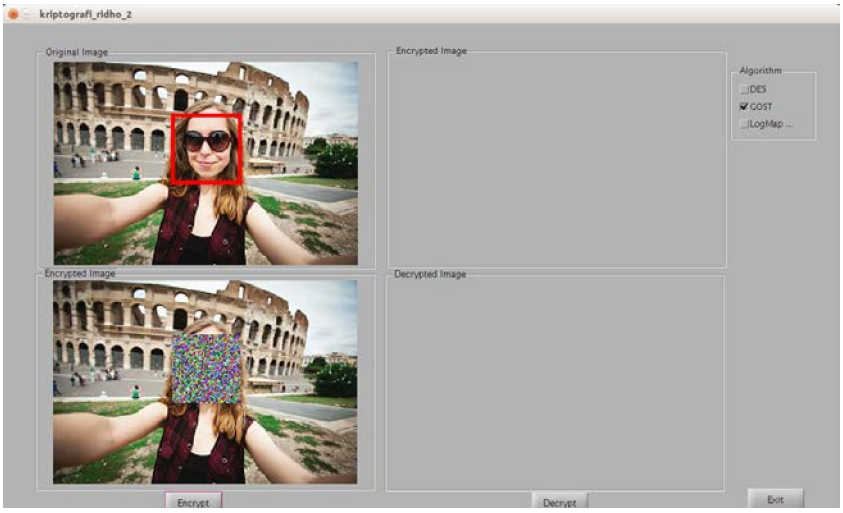

Figure 5. Rearranging pixel into original image and showed the result of encrypted image

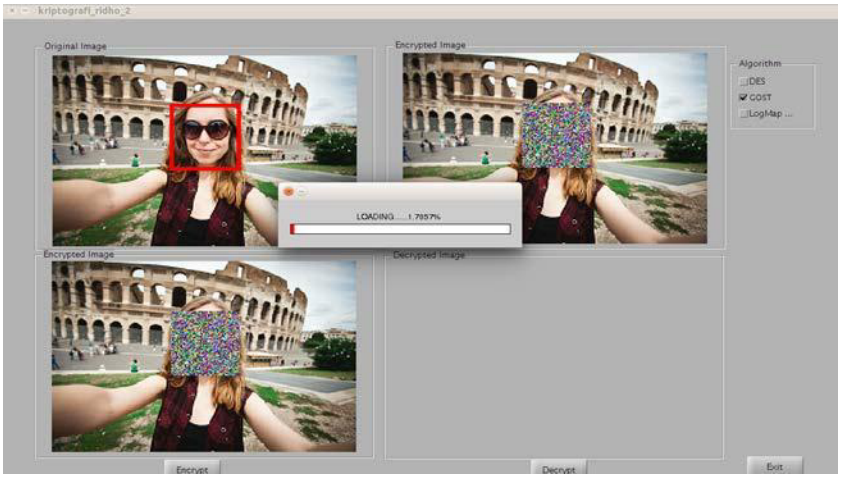

Figure 6. Uploading coordinates and encrypted image for input of decryption process.

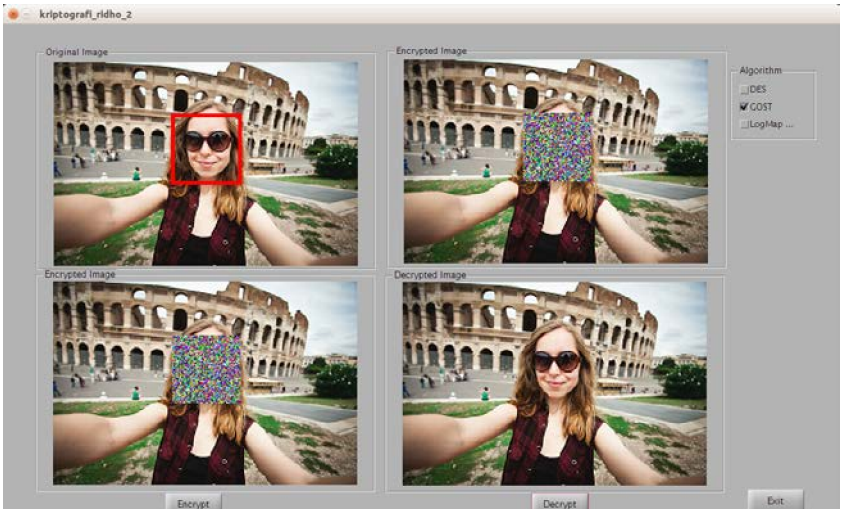

Figure 7. Result of decrypting process and rearranging of pixels

Graphics user interface of simulation is run in Matlab 2012 with Linux operating system and hardware specification Intel Core i3-2356M 1.40 GHz, installed RAM 3.87GB. Image with format .bmp (33x73 Pixel, 24 bit depth) has been tested, encrypted and decrypted

successfully with algorithm DES, GOST and logistic map – one time pad, calculated average time processing of encryption which showed at table 1.

Table 1. Comparison time processing between DES, GOST and logistic map — one time pad.

Algorithm	DES	GOST	Logistic map – One time pad
Processing speed (Pixel/second)	4.8150	5.5313	85702
Encryption time processing (second)	124.7029	183.2866	0.098226
Decryption time processing (second) (33x73 Pixel, 24 bit depth)	244.5134	371.2706	0.0865

CONCLUSION

Finally this simulation showed Viola and Jones Algorithm was suitable and also is working for detecting face on selfie photo. In other way, face detection make shorter of step for encrypting face in digital image. This method can be used well on block cipher algorithm or in cryptography based on chaos. Both of them (GOST and DES) still have relatively worst time processing (half an hour) for encrypting digital image. For implementing on mobile phone is recommended using logistic map – one time pad because has relatively better in time processing.

REFERENCES

1. Viola, Paul and Michael J. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 1, pp.511–518, 2001.
2. Federal Information Processing Standards Publication 46-3. Digital Encryption Standard (DES), U.S. Department of Commerence, National Institute of Standards and Technology, 1999.
3. GOST 28147–89. (1989). Cryptographic Protection for Data Processing Systems.
4. Bruce Schneier, Applied Cryptography, Second Edition, New York: Wiley, 1996.