IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VI (Sep – Oct. 2014), PP 01-03
www.iosrjournals.org

Password-oriented Image Encryption with multiple dependent factors.

Ishaan Agarwal[1]
[1]*Don Bosco Liluah, India*

Abstract: *The goal of this project was to develop a password-based image encryption algorithm that would be virtually safe from brute-force attacks, resulting in an image that would have no recognizable pattern. The algorithms designed were implemented in a java program. To increase the security of the algorithm, dual encryption keys generated based on the user's password are used and have an increased number of factors dependent upon the password. Apart from the pixel values, the location of pixels and the number of cycles of encryption, which the image will undergo, are also based on the password entered.*
Keywords*: Image Encryption, RGB, Shifting, Image Entropy*

I. Introduction

The unearthing of the existence of several global surveillance programs and the increased frequency of hackers exploiting vulnerable networks and encryption algorithms makes this topic pertinent.

Steganography techniques being used to conceal data using images, are being detected and cracked. The (2,n) Visual Cryptography technique [1] can also be broken by few of the sharing parties and their shares can be changed in order to create an entirely different secret message.

Although innumerable text based encryption techniques exist, image based ones are scarce and they are not user password oriented, making it unappealing to the standard consumer.

Also, the SSL protocols used to secure the transfer of data online are usually removed behind the front-end servers making the data susceptible to leakage. [2]

The algorithm is significantly safer than existing image encryption techniques which have been proved to be breakable.[3] Also, any attempt to manipulate the image by altering RGB values, or change in the size of the image could render the image un-decryptable even with the password, protecting the information from being leaked.

II. Proposed Method

In this algorithm, the user is asked for a password that is of minimum 6 characters, to prevent brute force attacks, and then the password is used to generate two separate encryption keys. [4]

Image Encryption –

1. Input valid image and password
2. Generate two encryption keys using SHA512 and MD5 algorithms
3. The image is broken up into dynamic blocks of pixels and passed on to other functions to encrypt or decrypt
4. The entire process is repeated a number of times based on the encryption keys.

Encryption and Decryption -

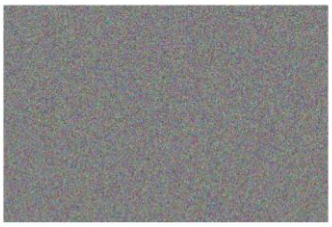
1. The characters of the encryption keys are converted to numeric values by taking the ASCII values of the characters into consideration.
2. The Red, Green and Blue values are altered based on the numeric values obtained from the encryption keys.
3. The Red, Green and Blue values of the pixels are converted to fit in the range of 0-255.
4. The Red, Green and Blue values of pixels are interchanged and thus shifted both horizontally and vertically within the dynamic blocks based on the encryption keys.

III. Results

Original Image

Password - test5678

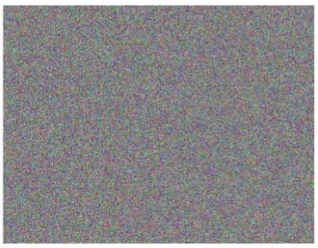
Encrypted Image



Original Image

Password - abcd1234

Encrypted Image



Original Image

Password - typewriter

Encrypted Image

The time taken to encrypt and decrypt an image depends upon the size of the image as well as the password entered since the number of iterations of encryption undergone by the image is also dependent on the user password. The average time, with computer with 2.26 Ghz Intel core 2 duo processer, for a high definition image is less than 4 seconds. The average time reduces if the number of iterations of encryption is slightly lowered.

An increased number of factors dependent on the password leads to a much more secure encryption technique.

All the test cases show extremely high visual degradation of the encrypted images, with no similarities to the original images. After decryption, the images are identical to the original images. Also, the encrypted images show no increase in image size compared to the original images making them optimal for storage.

V. Implementation

The main equipment used was a MacBook Pro, with a 2.26 Ghz Intel Core 2 Duo processer, running OS X Mavericks. The program was written in java and BlueJ Development Environment was used.

IV. Conclusion

Brute force attacks are not practically possible and the encrypted images are secure from being broken.The encryption algorithm can be used for a wide variety of purposes ranging from being commercially used by theconsumer to encrypt data for communication or storage to corporate houses handling business secrets to militaries dealing with classified information. The algorithm also presents future scope of modification to accommodate the encryption of videos using similar principals as used above.

References

[1] Feng Liu and ChuanKun Wu, Optimal XOR based (2,n)-Visual Cryptography Schemes,International Association for Cryptologic Research, 2010, 545.

[2] Gellman, Barton; Soltani, Ashkan(November 1, 2013),"NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say",The Washington Post.

[3] Jolly Shah and Dr. VikasSaxena, Performance Study on Image Encryption Schemes, International Journal of Computer Science Issues, Vol. 8, Issue 4, No. 1, July 2011.

[4] Paar, Christof; Pelzl, Jan; Preneel, Bart (2010).Understanding Cryptography: A Textbook for Students and Practitioners. Springer. ISBN 3-642-04100-0.