ENCRYPTING IMAGES WITH SQBC

V. Dimitrova Z. Trajcheska M. Petkovska
Faculty of Computer Science and Engineering
Skopje, Republic of Macedonia

ABSTRACT

The current trends impose storing almost all data digitally. In particular, we are interested in sensible data, such as personal data. Considering the latest tendencies, this data often is an image of some kind. We want to be sure that this type of data is not accessible in its original form, so that it would not be potential subject of manipulation. For the purpose of protecting the mentioned data, we should encrypt the image. This paper contains the results of the research conducted which refers to encrypting images in *.bmp format with the SQBC (Small Quasigroup Block Cipher). SQBC is a block cipher based entirely on quasigroups and quasigroup transformations. For experiments in our investigation we used small quasigroups of order 4.

I. INTRODUCTION

Consider SQBC as a family of block ciphers which utilize quasigroup transformations that provide encryption of a plaintext message into a cipher text using a working key generated form a secret key [1]. Also, a given cipher text can be decrypted to obtain the original message. The design of the SQBC is very flexible. We can choose different level of security and different kind of performances. The type of encryption of images is widely used in small devices or microchips that require the use of light weight cryptography, so for the purpose of this research we are using quasigroups of order 4. This way, memory or complexity problems can be avoided.

Previously conducted results [2] show that quasigroups can be partitioned to two categories: fractal and non-fractal quasigroups. Also, there is another classification of quasigroups: linear, non-linear and purely non-linear quasigroups by Boolean representation [7]. The experiments for encrypting an image with this cipher were done with quasigroups of all categories, so that we can see if the result depends on the type of quasigroup. We are trying to observe how "scrambled" will the encrypted image be. Intuitively, patterns in the encrypted image should be avoided.

The encryption and decryption of the images was automated using the implementation of SQBC in Java [3]. The source code was slightly modified in order to adjust it to encrypting and decrypting images in *.bmp format and to facilitate the process.

II. METHODS

To begin with, the collection of analyzed images were all in *.bmp format. Experiments will be also conducted with other image formats. It is important to understand how the *.bmp format is organized. Specifically, here we examine the 24-bit Bitmap images. The organization of the 24-bit Bitmap file roughly contains Bitmap File Header, Bitmap Info Header, RGBQuad array and color-index array [4,5]. The structure of the *.bmp file is shown in Table 1.

Table 1: Bitmap file structure

Name	Size	Description
Header	14 bytes	Windows Structure: Bitmap File Header
InfoHeader	40 bytes	Windows Structure: Bitmap Info Header
RGBQuad array	4 bytes	
color-index array	varies	

The Bitmap header (Header and InfoHeader) of 54 bytes is not encrypted since the data it contains is not directly related to the content of the image, but it represents the meta-data about the type of the file, width, height and other information for which there is no need for encryption. What we want to be encrypted is the very content of the image.

The image is encoded with Windows-1251 encoding, which is typical for this image format. To avoid problems with conversion, we take the input string as bit string. So, the input to the cipher is a string of bits, which are encrypted with SQBC and the resulting string is converted to hexadecimal and stored into a new file which contains the same header and the encrypted data.

Several quasigroups were included in the testing. The quasigroups are chosen from the classification elaborated in [2] and [7]. Also, their left and right parastrophe is used in the algorithm. For the fractal linear quasigroups we chose the quasigroup number 1, and for the non-fractal non-linear quasigroups we chose the quasigroup number 158. For the linear by Boolean representation quasigroups we chose number 576 as a representation and for the non-linear by Boolean representation the quasigroup number 575. Both quasigroups number 575 and 576 are fractal also. For the purely non-linear and non-fractal quasigroups we chose quasigroup number 181. As a representation of non-fractal linear quasigroups, we use quasigroup number 6. For the encryption using 128 bit block the results of the experiments were similar to each other, so we will show the images for the quasigroups 1 and 181 as most representative.

The secret key that was used for encryption was 11001111010001110110010101100111011010110110110101111100010111111111000001110001001, but this does not mean much as the key can be every bit string longer than 80 bits. The experiments were conducted using 10 rounds and a single round. The block length was taken to be 128, 24, 16 and 8 bits. In the 24-bit Bitmap [6] file the information for a single pixel is stored in 24 bits, the first 8 ones to represent the red color, the second 8 bits to represent the green color and the last 8 bits to represent the green colour. This is the reason we experimented with block length of 24 bits. We also did the encryption using 8 bit block to observe the result encrypting blocks of a single color of the pixel. We use 16 bit

block to see if the encrypted images are better if we encrypt blocks of two colors of the pixel or two consecutive pixels.
The first part of the experiments was conducted using a CBC (Cipher Block Chaining) block-cipher mode, and the other part was done with the simplest ECB (Electronic Codebook) block-cipher mode. It is expected that some kind of pattern will appear using the second mode (ECB) as it is far more simple that the first one (CBC).
The results of the encryption are represented as images, as well.

III. Experimental results

A. Results of the experiments using the CBC mode

The experiments were conducted using several pictures. From the first results, all of the encrypted images were intensely "scrambled" and no pattern appeared.
First, on Figure 1 we have a standard *.bmp picture. Figure 2 shows its encryption with the quasigroup number 181 and 128 bit blocks and Figure 3 the same with quasigroup 1.

Figure 1: The original image (1).

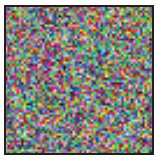

Figure 2: Encryption of (1) with the quasigroup number 181.

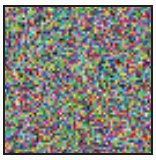

Figure 3: Encryption of (1) with the quasigroup number 1.

The results show that the encryption of the image so far doesn't depend on the quasigroup.

B. Results of the experiments using the ECB mode

Unlike the results from the previous experiments, here as expected a pattern appears. The same original pictures are used for the encryptions. In addition, we will show the results of the encryption.
The ECB mode is not as good as CBC mode as it only merges the encrypted blocks. So, the results of the encryption with ECB mode in general are not so good. So, we will use this mode to observe the impact of the quasigroup on the encryption. Instead of using the original concept of the SQBC algorithm [1], were the first block is encrypted differently than all the other blocks, we are using the algorithm for encrypting the first blocks for all the blocks from the input bit string.

Figure 4 shows the encryption of (1) with the quasigroup number 1 using blocks of 8, 16 and 24 bits respectively. Quasigroup number 1 is a fractal, linear quasigroup, so a pattern might appear.

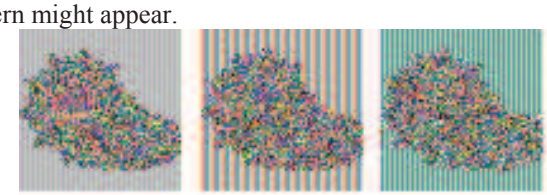

Figure 4: Encryption of (1) with the quasigroup number 1.

Here, we can easy recognize that a vertical line pattern appears whenever the input bit string is periodical. In Figure 4, we can see that the white background is striped and the rest is "scrambled". It seems that the non-periodical part of the image is quite "scrambled", but if we look closely we can see some small fractals and lines appear, especially when we use block length of 8 bits.
Figure 5 shows the encryption of (1) with the quasigroup number 6 using blocks of 8, 16 and 24 bits respectively. Quasigroup number 6 is a non-fractal, linear quasigroup.

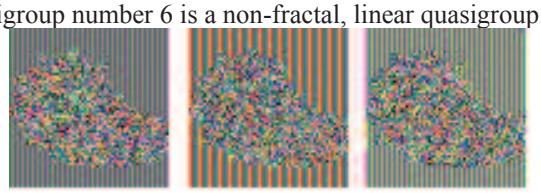

Figure 5: Encryption of (1) with the quasigroup number 6.

Again, very similar vertical line pattern appears whenever the input bit string is periodical as in the white background of the original image, but no significant pattern appears in the non-periodical part of the image.
Figure 6 shows the encryption of (1) with the quasigroup number 158 using blocks of 8, 16 and 24 bits respectively. Quasigroup number 158 is a non-fractal, non-linear quasigroup.

Figure 6: Encryption of (1) with the quasigroup number 158.

Figure 7 shows the encryption of (1) with the quasigroup number 181 using blocks of 8, 16 and 24 bits respectively. Quasigroup number 181 is a non-fractal, purely non-linear quasigroup.

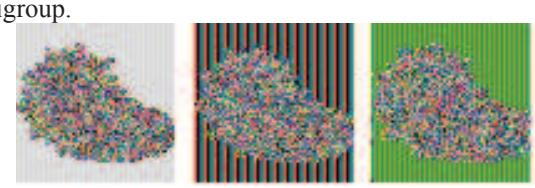

Figure 7: Encryption of (1) with the quasigroup number 181.

Figure 8 shows the encryption of (1) with the quasigroup number 575 using blocks of 8, 16 and 24 bits respectively. Quasigroup number 575 is a fractal, non-linear quasigroup.

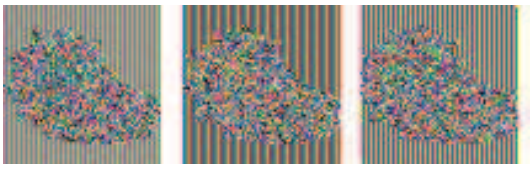

Figure 7: Encryption of (1) with the quasigroup number 575.

Figure 8 shows the encryption of (1) with the quasigroup number 576 using blocks of 8, 16 and 24 bits respectively. Quasigroup number 576 is a fractal, linear quasigroup.

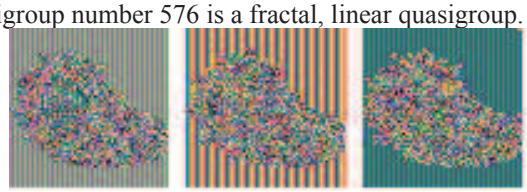

Figure 8: Encryption of (1) with the quasigroup number 576.

This shows that the CBC mode is far more convenient for the use of encrypting images with SQBC than the ECB mode.

Also, the original image (1) was encrypted using 8 bit block and ECB mode, with the original concept of the SQBC algorithm [1] where the first block is encrypted with one and all other blocks with another algorithm. The quasigroups used were quasigroup number 1, quasigroup number 6 and quasigroup number 181. Figure 9 shows the results.

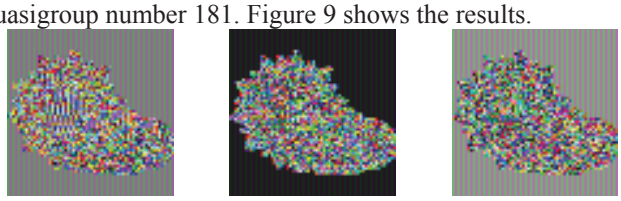

Figure 9: Encryption of (1) with the quasigroup number 1 and 181, using ECB mode and the SQBC algorithm.

All encryptions had some small fractal structures, especially noticeable the one encrypted with quasigroup number 1.

IV. Conclusion

The first results in this ongoing research were good, so we could extend it. We made a lot of experiments with different quasigroups and different block-cipher modes and we can conclude that for some quasigroups encrypted images have fractal structures. We will expand to researching other image formats and study the results using a bigger set of quasigroups and the automated process will be upgraded.

Further more, currently these experimental results are theoretically observed and will be hopefully theoretically proven.

V. Acknowledgements

We would like to thank Prof. Dr. Smile Markovski for the useful comments and guidelines for this research.

References

[1] S. Markovski, V. Dimitrova and A. Mileva, "*SQBC - Block Cipher Defined by Small Quasigroups*", Loops'11, 2011

[2] V. Dimitrova, "*Quasigroup transformations and their applications*", MSc Thesis, Skopje, 2005

[3] Z. Trajcheska, M. Petkovska, M. Kostadinoski and G. Velkoski: *Implementation of SQBC in Java*, FCSE, Skopje, 2012

[4] MSDN Library, Bitmaps, Bitmap Storage, *http://msdn.microsoft.com/en-us/library/dd183391(v=vs.85).aspx*

[5] D. Lancaster, "*Exploring the .BMP File Format*" ©2003 as GuruGram #14, *http://www.tinaja.com/glib/expbmp.pdf*

[6] Alyce Watson, "*Bitmap Color Formats (intermediate level)*" © 2002, http://www.libertybasicuniversity.com/lbnews/nl100/format.htm

[7] D. Gligoroski, V. Dimitrova, S. Markovski: "*Quasigroups as Boolean functions, their equation systems and Groebner bases*", "Groebner Bases, Coding, and Cryptography", Ed. T.Mora, L.Perret, S.Sakata, M.Sala, and C.Traverso, Springer Berlin Heidelberg, 2009, pp. 415-420.