An Approach for Secured Transmission of Data using Fractal based Chaos

Jyotsna Shaw
Student
Department of Computer Science & Engineering
Jadavpur University
Kolkata-700032, India

Olivia Saha
Student
Department of Computer Science & Engineering
Jadavpur University
Kolkata-700032, India

Atal Chaudhuri
Professor
Department of Computer Science & Engineering
Jadavpur University
Kolkata-700032, India

ABSTRACT

Cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. This paper presents an innovative concept on Encryption/Decryption application that is able to work with image files, data files and audio files. The method of encryption is simple but competent enough to fit the needs of the day. This paper presents Chaos based cryptography where the chaos is generated by using the concept of Fractals .The technique uses a key of variable length which generates a 128 bit message digest using MD5 hash algorithm. Then the generated hash value used as a seed to generate fractals using Julia Set algorithm and this is used as a chaos for the respective files. The final encryption is performed through XOR operation on each block of data to generate the cipher file which is to be transmitted.

General Terms

Cryptography and Data Security.

Keywords

Fractals, Cryptography, Julia Set, MD5.

1. INTRODUCTION

Cryptography is the study of Secret (crypto-)-Writing (-graphy).It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then transforming the message back to its original form. Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm.

This scheme uses a powerful encryption algorithm. The strength of cryptography lies in the choice (and management) of the keys as longer keys will resist attack better than shorter keys [16] hence in this scheme in the first level of security, a secret key of variable length generates a 128 bit message digest using MD5 algorithm[3] which is very complex to break. The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number. MD5 is a one way hash function that works in one direction but not in the other. This means that it is very easy to compute a hash value from a pre-image and very difficult to compute the pre-image from a certain hash value. A good one-way hash function is also collision free. This means that it is hard to find two pre-images with the same hash value. So we have used this unique feature in our scheme to make the key more secure. This makes the algorithm more confused and thus it becomes more robust since the intruders cannot guess the size of the key.

In the second level it uses a more powerful encryption algorithm in which fractals are used as chaos to generate cipher file. This scheme uses fractal to create chaos due to its unique features such as irregularity and chaotic nature. The key used in this method is used in generating fractals and thus is chaotic in nature which provides more confidentiality against the intruders to manipulate the key and is obviously resistant to cryptanalysis.

The technique allows the sender to enter a secret key of variable length with a fixed lower limit but no upper limit which generates a 128 bit message digest using MD5 algorithm[4][5]. The hash value so generated is used as a seed for generating fractal [6] [7] using Julia set algorithm [8]. This fractal is used as a chaos for data files. The fractal file is XOR-ed [8] with the plain text to create the encrypted cipher file.

This scheme provides strong protection at the encryption phase but the computational complexity is very low. Moreover, it is simple, so applicable to various applications with low end processors on hand held system.

2. RELATED WORK

A fractal is a mathematical set that has a fractal dimension that usually exceeds its topological dimension and may fall between the integers. Fractals are typically self-similar patterns, where self-similar means they are "the same from near as from far". Fractals were first described in the 1970s by IBM mathematician Benoit Mandelbrot. He found traditional geometry to be incomplete. It could not describe the enormous and irregular shape of a mountain. It had no formal representation of the appearance of a cloud. The new geometry that he developed could do all this. It was a description of the beautiful yet irregular and fragmented patterns around us.

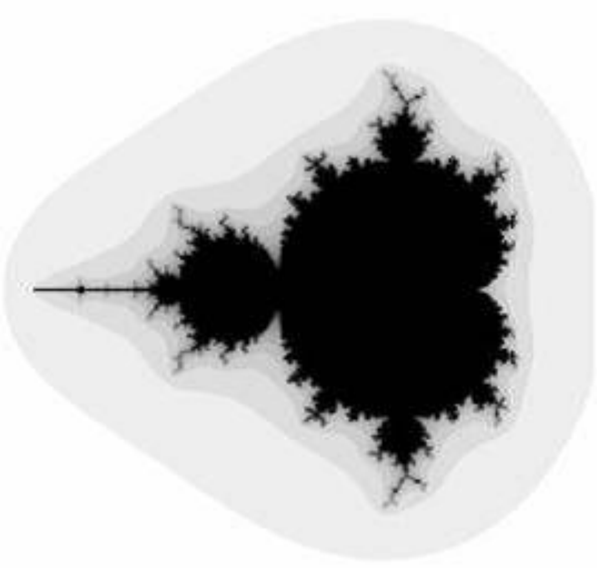


Fig. 1: Fractal generated with the Mandelbrot set.

The term 'fractal' was coined by Mandelbrot from the Latin fractus, an adjective for the irregular and the fragmented. Essentially, they replicate themselves by fragmentation.

What is a Julia Set:

Julia studied rational polynomial expressions of various degrees (e.g., z4 + z3/(z + 1) + z2/(z3 + 4z2 + 5)+ c), but in this project we have limited the work mostly to the family of sets generated by the special quadratic case form f(z) = z2 + c. Here z represents a variable of the form a+ib (a and b real numbers) which can take on all values in the complex plane. The quantity c also is defined as a complex number, but for any given Julia set, it is held constant (thus it is termed a parameter).

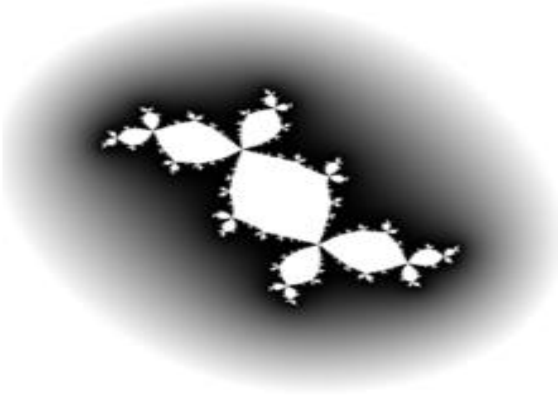


Fig. 2: Potential of filled Julia set

Chaos Theory has been established since 1970s in many different research areas, such as physics, mathematics, engineering, and biology. The most well known characteristics of chaos are the so called "butterfly-effect" (sensitivity to initial conditions), and the pseudo-randomness generated by deterministic equations [20]. (Many fundamental properties of chaotic systems have their corresponding counterparts in traditional cryptosystems. Chaotic systems have several significant features favorable to secure communications, such as sensitivity to initial conditions, control parameters and random like behavior [21].

With all these advantages, scientists expected to introduce new and powerful tools of chaotic cryptography. So, chaos may become a new rich source of new ciphers.

3. PROPOSED WORK

3.1 Concept

3.1.1 Encryption Process

The proposed scheme uses symmetric key algorithm. This means that the sender and the receiver will use the same key for encryption and decryption process. At first the algorithm creates a fixed 128bit length of MD5 hash value from the variable length key entered. The hash value so generated is used as a seed for generating fractal using Julia set algorithm. This fractal is used as a chaos for input data file .After fractal is being generated, XOR based encryption algorithm is used where each and every byte of original data file is XORed with individual byte of the constructed fractal image which in turn produces a chaotic file known as cipher file. This cipher file is to be transmitted where the original information of the data file is being ciphered.

3.1.2 Decryption Process

In the decryption phase, the receiver receives the cipher file. He enters the same key communicate securely earlier and generates a 128-bit message digest using MD5 algorithm. Then this generated hash value is used as a seed to generate fractal using Julia Set algorithm. After this, the generated fractal is XORed with the cipher file to get back the original data file that is being transmitted. However if the receiver enters a different key then it will not produce the same hash value. Thus the fractal generated will be different and when it is being XORed with the cipher file, it will fail to decrypt the original data file.

3.1.3 Algorithm

3.1.3.1 Encryption Phase

This scheme is applied for any data file which we want to transmit over the network. The algorithm to encrypt the file can be described by the following algorithm:

Step1: Select any data file which is to be transmitted.

Step2: Enter a secret key of variable length with a lower limit (we have taken 10) but no upper limit.

Step3: Evaluate the hash value of the entered key using MD5 algorithm ultimately to make it to 128 bit. This makes the algorithm more confused and thus it becomes more robust since the man in the middle cannot guess the size of the key.

Step4: The hash value so generated is used as a seed for generating fractal using Julia set algorithm.

Step5: This fractal is used as a chaos for data file. The fractal is XORed byte by byte with the original data file to generate the encrypted cipher file.

3.1.3.2 Decryption Phase

The algorithm to decrypt the transmitted file can be described as follows:

Step1: Take any chaosed encrypted cipher file.

Step2: Enter the secret key.

Step3: Evaluate the hash value of the entered key using MD5 algorithm ultimately to make it to 128 bit.

Step4: The hash value so generated is used as a seed for generating fractal using Julia set algorithm.

Step5: Now the generated fractal file is XORed byte by byte with the selected cipher file to get back the original file.

3.2 Data Analysis with SNR Value

Signal-to-noise ratio (often abbreviated SNR or S/N) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise.

Data Analysis with SNR values of cipher files with respect to the original files of the above proposed scheme are as follows. In cryptography higher the values better the confusion. Fig 3 shows in this case is always above 99% i.e. both known text attack and blind text attack are impossible.

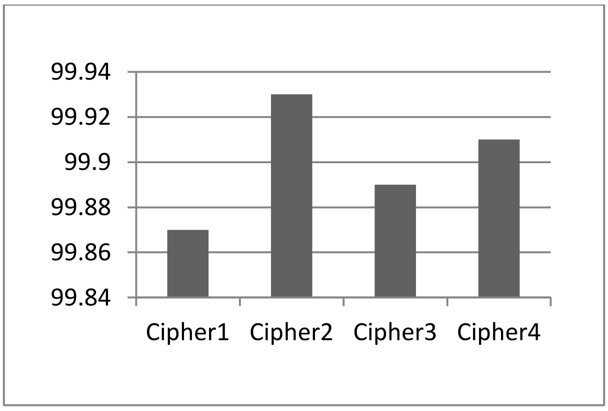


Fig. 3: Data Analysis with SNR Value

3.3 The Advantages of Proposed System

Since the key size of any arbitrary length is transformed into a 128 bit hash value thus it takes 8 trillion millennia time to search 50% of the key space. This makes the algorithm more confused and thus it becomes more robust since intruders cannot guess the size of the key.

The formula of Fractal transformation is one-way. By changing the parameters of the formula, different fractals are generated. Hence the proposed encryption algorithm confirms confidentiality and security and is highly useful where low end processors are used but security is a major challenge.

The generation of chaos using fractal generation creates confusion for the intruders and thus diffusion of information is less for cryptanalysis.

3.4 Input and Output Example with GUI

3.4.1 GUI of the Proposed Scheme

3.4.1.1 Encryption Phase

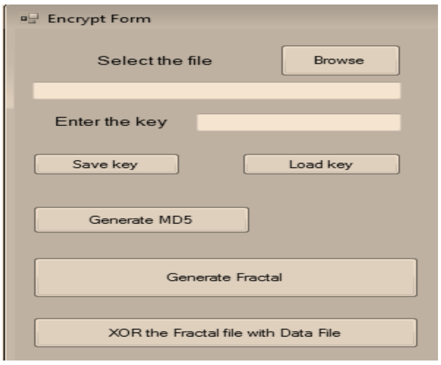
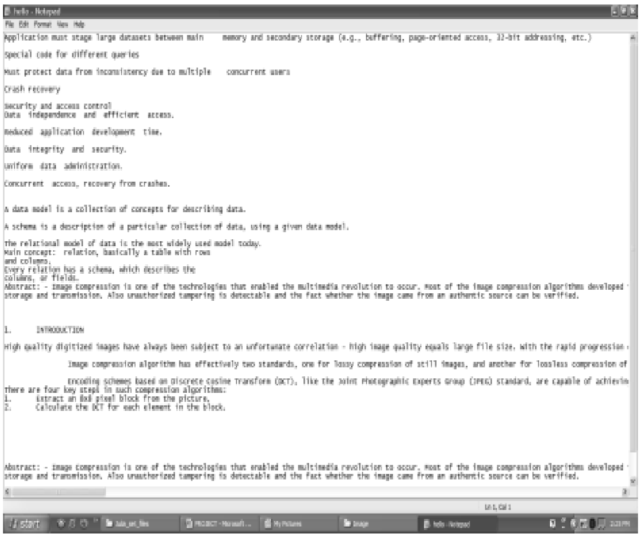


Fig. 4: GUI of the Encryption Phase



```
Application must stage large datasets between main     memory and secondary storage (e.g., buffering, page-oriented access, 32-bit addressing, etc.)

Special code for different queries

Must protect data from inconsistency due to multiple    concurrent users

Crash recovery

Security and access control
Data  independence  and  efficient  access.

Reduced  application  development  time.

Data  integrity  and  security.

Uniform  data  administration.

Concurrent  access, recovery from crashes.


A data model is a collection of concepts for describing data.

A schema is a description of a particular collection of data, using a given data model.

The relational model of data is the most widely used model today.
Main concept:  relation, basically a table with rows
and columns.
Every relation has a schema, which describes the
columns, or fields.
Abstract: - Image compression is one of the technologies that enabled the multimedia revolution to occur. Most of the image compression algorithms developed
storage and transmission. Also unauthorized tampering is detectable and the fact whether the image came from an authentic source can be verified.



1.      INTRODUCTION

High quality digitized images have always been subject to an unfortunate correlation - high image quality equals large file size. With the rapid progression

              Image compression algorithm has effectively two standards, one for lossy compression of still images, and another for lossless compression of

              Encoding schemes based on Discrete Cosine Transform (DCT), like the Joint Photographic Experts Group (JPEG) standard, are capable of achievin
There are four key steps in such compression algorithms:
1.      Extract an 8x8 pixel block from the picture.
2.      Calculate the DCT for each element in the block.





Abstract: - Image compression is one of the technologies that enabled the multimedia revolution to occur. Most of the image compression algorithms developed
storage and transmission. Also unauthorized tampering is detectable and the fact whether the image came from an authentic source can be verified.
```

Fig. 5: Input Text File/ Message to be sent and thus encrypted

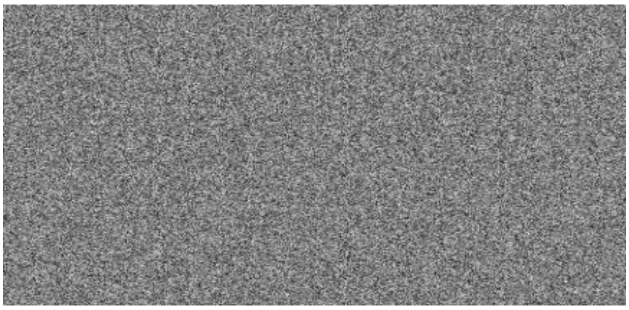


Fig. 6: Cipher file

3.4.1.2 Decryption Phase

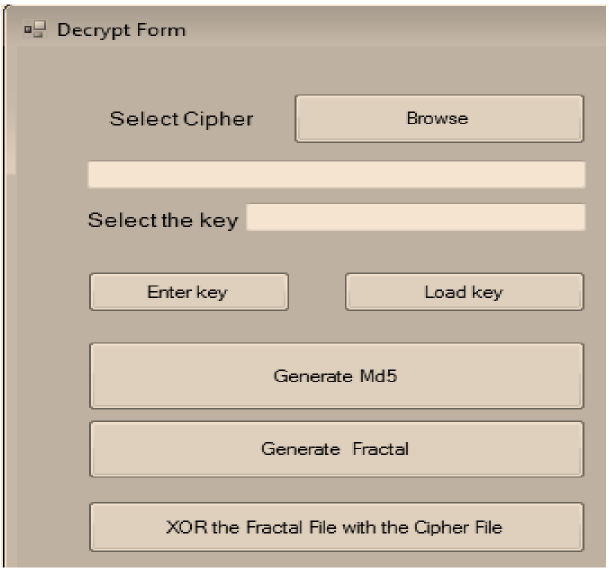
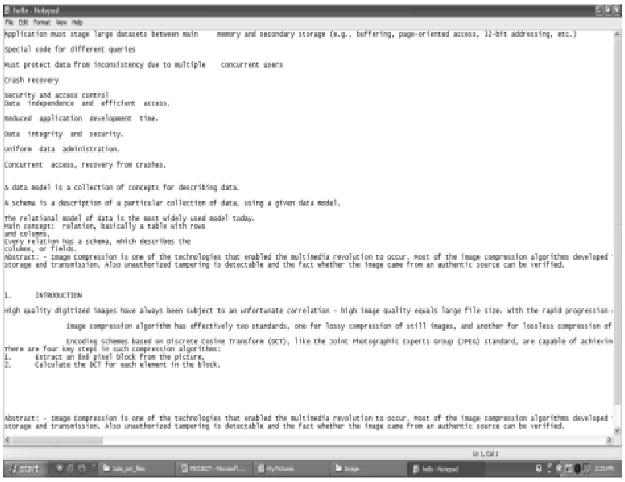


Fig. 7: GUI of the Decryption Phase



```
Application must stage large datasets between main    memory and secondary storage (e.g., buffering, page-oriented access, 32-bit addressing, etc.)

Special code for different queries

Must protect data from inconsistency due to multiple    concurrent users

Crash recovery

Security and access control
Data  independence  and  efficient  access.

Reduced  application  development  time.

Data  integrity  and  security.

Uniform  data  administration.

Concurrent  access, recovery from crashes.


A data model is a collection of concepts for describing data.

A schema is a description of a particular collection of data, using a given data model.

The relational model of data is the most widely used model today.
Main concept:  relation, basically a table with rows
and columns.
Every relation has a schema, which describes the
columns, or fields.
Abstract: - Image compression is one of the technologies that enabled the multimedia revolution to occur. Most of the image compression algorithms developed
storage and transmission. Also unauthorized tampering is detectable and the fact whether the image came from an authentic source can be verified.


1.      INTRODUCTION

High quality digitized images have always been subject to an unfortunate correlation - high image quality equals large file size. With the rapid progression

               Image compression algorithm has effectively two standards, one for lossy compression of still images, and another for lossless compression of

               Encoding schemes based on Discrete Cosine Transform (DCT), like the Joint Photographic Experts Group (JPEG) standard, are capable of achievin
There are four key steps in such compression algorithms:
1.      Extract an 8x8 pixel block from the picture.
2.      Calculate the DCT for each element in the block.




Abstract: - Image compression is one of the technologies that enabled the multimedia revolution to occur. Most of the image compression algorithms developed
storage and transmission. Also unauthorized tampering is detectable and the fact whether the image came from an authentic source can be verified.
```

Fig. 8: Text file / Message Output after Decryption

4. CONCLUSION

This scheme have introduced a new robust and fractal based cryptography scheme which provides a good, efficient method for hiding the data from intruders and sent to the destination in a safer manner. This proposed system will not change the size of the file even after encoding. The Encryption and Decryption techniques have been used to make the system more secure and robust.

This scheme is a better cryptography scheme because it not only confirms confidentiality but also provides strong protection of the secret file at the decryption phase. The basic idea behind this paper is to provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power during the encryption and decryption phases for low end processor in hand held system.

5. ACKNOWLEDGMENTS

We would like to express our grateful thanks to all lab assistants of computer science department for providing us lab facility as an when required.

6. REFERENCES

[1] G.R. Blakley, “Safeguarding cryptographic keys,” AFIPS Conference Proceedings, vol.48, pp.313–317, 1979.

[2] M. Naor and A. Shamir, ³Visual cryptography,´ Advances in Cryptography-EURO CRYPT 94,Perugia, Italy, pp. 1-12, May 1994.

[3] H. Dobbertin. Cryptanalysis of MD5 compress, presented at the rump session of Eurocrypt’96.

[4] R.L. Rivest. The MD5 message-digest algorithm, Request for Comments (RFC 1320), Internet Activities Board, Internet Privacy Task Force, 1992.

[5] http://en.wikipedia.org/wiki/MD5

[6] P. Davern and M. Scott. Fractal based image. Information Hiding, First International Workshop, Lecture Notes in Computer Science, pages 279–294, 1996.

[7] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. In Proceedings of SPIE Photonics East’96 Symposium, Boston, Massachusetts, 1996.

[8] Andy Wilson, “Tips and Tricks: XOR Encryption” http://www.andyw.com/director/xor.asp,1998.

[9] Threshold Cryptography Based on Blakley Secret Sharing,˙Ilker Nadi Bozkurt, Kamer Kaya, Ali Aydın Selc¸uk

[10] C. Asmuth and J. Bloom. A modular approach to key safeguarding. IEEE Trans. Information Theory, 29(2):208–210, 1983.

[11] William Stallings, “Cryptography and Network Security, Principles and Practice”, Third Edition, Pearson education, 2005

[12] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. In Proceedings of SPIE Photonics East’96 Symposium, Boston, Massachusetts, 1996.

[13] E. Biham, A. Shamir. Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[14] H. Dobbertin. Cryptanalysis of MD5 compress, presented at the rump session of Eurocrypt'96.

[15] R.L. Rivest. The MD5 message-digest algorithm, Request for Comments (RFC 1320), Internet Activities Board, Internet Privacy Task Force, 1992.

[16] Wikipedia,"Encryption", http://en.wikipedia.org /wiki/Encryption, modified on 13 December 2006.

[17] Freeman J., Neely R., and Megalo L. "Developing Secure Systems: Issues and Solutions". IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998

[18] Andy Wilson, "Tips and Tricks: XOR Encryption" http://www.andyw.com/director/xor.asp,1998.

[19] Di_e, W., and Hellman, M. New directions in cryptography. IEEE Trans. Inform.Theory IT-22, (Nov. 1976), 644-654.

[20] G. Jakimoski and L. Kocarev, Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 48, No. 2, pp. 163-169, February 2001.

[21] K. Kelber and W. Schwarz, General Design Rules for Chaos-Based Encryption Systems , International Symposium on Nonlinear, Theory and Its Applications (NOLTA2005), pp. 465-468, Bruges, Belgium, 18-21 October, 2005.