Chapter 3
History, Development and Trend of Fractal Based Biometric Cryptography

Md Ahadullah, Mohamad Rushdan Md Said and Santo Banerjee

Abstract This article has been originated to institute for obtaining the History and the trend of Development of Fractal based Biometric Cryptography. Here we endeavour to assemble the bygone information for representing the trend of progress of cryptography operated with the perception of Fractal. On a whole, Fractal is a geometric figure of non-integer dimension that has two properties: First, most amplified images of fractals are approximately identical from the unamplified version, called self-similarity. Second, fractals have fractional dimensions. Barnsley's Iterated Function Systems (IFS) form on the self-similarity of fractal sets can produce the Fractal Image Coding Scheme by using the principle of affine transformation. To encode digital grey level images, Fractal image coding has been used successfully.

Keywords Fractal · Encryption · Fractal image

3.1 Introduction

This article has furnished a brief background, Progress and trend of Biometric Cryptography based on Fractal.

Different Bodily features are measured as a method of distinct identity is known to date back to the ancient Egyptians. Archaeological evidence says that fingerprints being used to associate a person with some event or transaction is also said to date

M. Ahadullah (✉) · M.R.M. Said · S. Banerjee
Institute for Mathematical Research (INSPEM), University Putra Malaysia,
UPM, Serdang 43400, Selangor Darul Ehsan, Malaysia
e-mail: md.ahad1234@gmail.com

M.R.M. Said
e-mail: mrushdan@upm.edu.my

S. Banerjee
e-mail: santoban@gmail.com

Ş.Ş. Erçetin and S. Banerjee (eds.), *Chaos, Complexity and Leadership 2013*,
Springer Proceedings in Complexity, DOI 10.1007/978-3-319-09710-7_3

back to ancient China, Babylonia and Assyria. But until the end of the 19th century, the study of biometrics did not enter the domain of crime detection. A French police clerk, Alphonse Bertillon and anthropologist pioneered a method of recording multiple body measurements for criminal identification purposes known as Bertillonage was adopted by many police authorities worldwide during the 1890s, but soon became obsolete once it was recognized and thus the requirements of the encryption of body Image had become crucial (Alarcon-Aquino 2011; Alfalou et al. 2011; Alfalou and Brosseau 2009; Al-Saidi and Said 2014).

Mandelbrot, in the 1970s, devised the term fractal and originated the inception of 'Fractal Geometry' from 1975 but stipulated that objects now considered as fractal prevailed long before that decade. During formulation of the word fractal, Benoit Mandelbrot mentioned, "I coined fractal from the Latin adjective fractus. The corresponding Latin verb frangere means to break to create irregular fragments. It is therefore sensible and how appropriate for our needs!—that, in addition to fragmented, fractus should also mean irregular, both meanings being preserved in fragment."The theory, fractals is an active branch of nonlinear science starting from the 1970s become modern practice in Biometric Cryptography and attempt a new approach to enquiry the self-similarity objects and irregular phenomena. For its suitable applications in many fields particularly in image processing, Fractal has been accepted as a convinced technology in the world of Cryptosystem. Euclidean geometry fails to explain some geometrical structures whereas fractal geometry can interpret with. Fractal theory and its methodology provide people a new view and new idea which potentially be used in Biometric Cryptosystem (Al-Saidi and Said 2009; Alfaris et al. 2008).

Fractal geometry deals with objects in non-integer dimensions, at the same time the classical Euclidean geometry functions with objects which subsist in integer dimensions. Euclidean geometry is a illustration lines, circles, cuboids etc. Fractal geometry, regardless, is outlined in algorithms, a collection of instructions by what means to design a fractal.

Our world so as to appear is made up of objects which occur in integer dimensions, single dimensional points, one-two-three dimensional bodies. However, many things in nature are described better with dimension being part of the way between two whole numbers. While a straight line has a dimension of exactly one, a fractal curve will have a dimension between one and two, depending on how much space it takes up as it curves and twists. The more a fractal fills up a plane, the closer it approaches two dimensions. In the same manner of thinking, a wavy fractal scene will cover a dimension somewhere between two and three. Hence, a fractal landscape which consists of a hill covered with tiny bumps would be closer to two dimensions, while a landscape composed of a rough surface with many average sized hills would be much closer to the third dimension (Al-Saidi et al. 2011; Cavoukian and Stoianov 2011; Dang and Chau 2000).

Fractal Image storing based on image description in concise form of iterated function system is become possible because of Barnsley's Iterated Function Systems (IFS) form on the self-similarity of fractal sets. Barnsley's shows that numerous objects can firmly be estimated by self-similarity objects that can also be developed by the application of IFS transformations and thus the Biometric

Cryptosystem, a class of materealizing technologies, based on Fractal, can securely give birth to a digital key therefore no biometric image or template or digital key can be retrieved from the server.

Development in computer science and communications has been making demand to increase security system for last 20 years. In response to this demand, countywide security systems in computer science and communications have been improved by using modern cryptosystems. Thus the trend of development of Biometric Cryptosystem based on Fractal Image Coding Scheme is increasing and this is how seven major biometric technologies already been established as:

- Fingerprint recognition;
- Hand geometry recognition;
- Facial recognition;
- Iris and retina recognition;
- Voice recognition;
- Keystroke recognition;
- Signature recognition (Dhawan 2011; Das 2011; Gaddam and Lal 2010).

Brief History, Trend of Development of Biometric Cryptography based on Fractal Image Coding Scheme.

As only Biometric features in security aspect became obsolete meanwhile, the quest for a physical identifier that was unique to each individual gained significant ground when British anthropologist, Sir Francis Galton, worked on the principle that fingerprints were permanent throughout life, and that no two people had identical fingerprints. Galton calculated the odds of prints from two people being identical to be 1 in 64 billion and also identified characteristics known as minutiae that are still used today to demonstrate that two impressions made by the same finger match.

Galton's model provided the basis of the first fingerprint file established in 1891 by Juan Vucetich, an Argentine police officer, who became the first to use a bloody fingerprint to prove the identity of a murderer during a criminal investigation. In 1897, Sir Edward Henry, a British police officer serving as Inspector General of the Bengal Police in India, also developed an interest in the use of fingerprints for identifying criminals, even though the Bengal Police was at that time using Bertillonage. Based on Galton's observations, Henry and colleagues established a modified classification system allowing fingerprints captured on paper forms using an ink pad to be classified, filed and referenced for comparison against thousands of others. By 1901, Henry's fingerprinting system had been adopted in the UK by Scotland Yard and its use then spread through most of the world to become a standard method of identity detection and verification in criminal investigations (Jain and Karthik 2012; Jain et al. 2011; Kaur et al. 2010).

In the mid-1960s, the Royal Canadian Mounted Police (RCMP) adopted an automated video tape-based filing system allowing identification officers to make fingerprint comparisons on-screen. A similar 'Videofile System' was installed at New Scotland Yard in 1977. Around the same time, the USA's Federal Bureau of Investigation (FBI) was working with industry to build the first automated fingerprint card reader, which was implemented in 1974. Over the next 5 years, the FBI

and other organizations in Canada, Japan and the UK, developed further core technologies including fingerprint matching hardware, plus automated classification software and hardware. By the early 1980s, this culminated in the automatic fingerprint identification system (AFIS), which allowed the automatic matching of one or many unknown fingerprints against an electronic database of known prints; another major forward step in the world of crime detection and international security. Such systems have since reduced the manual capture, store, search and match processes for fingerprints from weeks and months, to hours and minutes, and have led to AFIS being deployed by law enforcement agencies in Europe and world-wide.

With the advent of computers and digital technology in the 1970s, fingerprinting took on a new dimension. As a result, the UK's fingerprint service now records 120,000 sets of fingerprints each year as volume of records that was simply untenable before computerization. Within a century, biometrics had evolved from tape measure, ink and pad techniques requiring vast manual filing and archiving resources, to an automated biometric digital scanning process using computerized storage, automated search and find/match techniques, plus extensive archiving and access systems with worldwide links. Such technology now provides for the capture and processing of biometrics information and has transformed fingerprinting techniques and procedures (Khan et al. 2007, 2005; Liu and Sun 2010).

But all this biometric process is converting Biometric Encryption process and we hope that all security system will depend on Biometric Encryption System 1 day and that is not so far.

3.2 Progress of Fractal Based Biometric Encription as a Commercial Commodities

The concept of Biometric Encryption (BE) was first introduced in the mid-90s by G. Tomko et al. Biometric Encryption is a process that securely binds a digital key to a biometric or generates a key from the biometric. The Acceptance for biometric airport scans has become very high after Malaysia Airlines disappearance. Many countries in the world now using biometric Encryption process in area such that: Crime and Fraud Prevention, Detection, and Forensics, Attendance Recording, Payment Systems, Access Control, Border Security Control. So all kind of developments, the technological, Research as well as commercial are proceeding in the same fashion.

3.3 How to Installed Fractal Geometry on Biometric Cryptography

The goal of FIC is to be able to store an image as a set of IFS transformation instead of storing individual pixel data. The local iterated function systems are used because we work on a section of the image instead of the whole image.

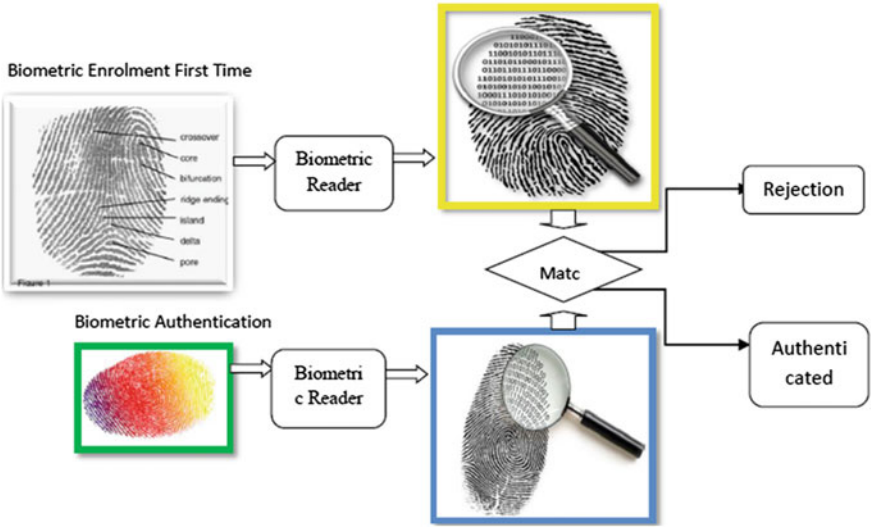

Fig. 3.1 Biometric enrolment and authentication diagram Secret key encryption

Fractal geometry deals with objects in non-integer dimensions, at the same time the classical Euclidean geometry functions with objects which subsist in integer dimensions,. Euclidean geometry is a illustration lines, circles, cuboids etc. Fractal geometry, regardless, is outlined in algorithms', a collection of instructions by what means to design a fractal.

In Fig. 3.1 it shows how Biometric enrolment and authentication system produce Secret key encryption.

3.4 Advantages of Biometric Encryption Over Other Biometric System

Technological Biometric Encryption approaches have extensive prospective to enhance privacy and security. The following are the key merits of this technology:

1. Memorizing of the biometric image or template is not required
2. Different level of identifiers as Multiple, cancellable and revocable
3. Authentication security enhanced much

- No substitution attack
- No tampering
- No masquerade attack
- No Trojan horse attacks
- No overriding Yes/No response

4. Personal data and communications secured more.
5. Public confidence, acceptance, and use are increasing; compliance with privacy laws is greater than before
6. For large-scale applications is very Suitable (Rahman 2010)

3.5 Conclusion

Biometric technologies surely add a modern degree of authentication and identification to applications, but risks and challenges are still here. There have crucial methodological confrontations such as perfection, authenticity, data defense, user consent, cost, and interoperability and overall provocations linked with certifying effective privacy protections. Security vulnerabilities of biometric systems include:

Spoofing; replay attacks; substitution attacks; tampering; masquerade attacks; Trojan horse attacks; and overriding Yes/No response.

Still the important of Identification and authentication are sharply increasing in both the online and offline worlds. Public and private sector entities are demanding to know who they are dealing with. The current security model for the verification of identity, protection of information, and authorization to access premises or services is based on using a token which allows access to information, premises or services. This modern token is a biometric (something you are). In this case, the details of the token is held by a third party whose function is to authorize and at times allow the transaction to proceed if the details of an individual's token match those stored in a database. The biometric is increasingly viewed as the ultimate form of authentication or identification, supplying the third and final element of proof of identity. Besides this Public key systems grounded on IFS transformation execute more actively than RSA cryptosystems in respect to key size and key space. So Biometric Encryption based on fractal iterative function system is very demanding. Accordingly, it is being rolled out in many security applications (Ratha et al. 2001; Shakhnarovich and Moghaddam 2011).

Though Biometrics has recently been awarding attention in popular media, it is extensively concluded that biometrics will be a momentous component of the identification technology as (i) the cost of biometrics sensors start to fall (ii) the root technology becomes more mature, and (iii) the public becomes appreciative of the strengths and limitations of biometrics. And laterally our expectation goes, in applications including Law enforcement, Banking, Security the usage of Biometric encryption will increase.

Unisys (www.Unisys.com) Surveys that Consumers worldwide support biometrics nearly 70 %.The Unisys research also found 66 % of consumers worldwide favored biometrics as the ideal method to combat fraud and identity theft as compared to other methods such as smart cards and tokens. In the future, no one will need pockets (Rathgeb and Uhl 2011; Sabena et al. 2010; Xi 2011).

References

Alarcon-Aquino V (2011) Biometric cryptosystem based on keystroke dynamics and k-medoids. IETE Journal of Research, Medknow Publications & Media Pvt. Ltd. 57

Alfalou A, Brosseau C (2009) Optical image compression and encryption methods. Adv Opt Photonics 1:589–636

Alfalou A et al (2011) Simultaneous fusion, compression, and encryption of multiple images. Opt Expr 19:24023–24029

Alfaris R, Ariffin MRK, Said MRM (2008) Rounding theorem the possibility of applying cryptosystems on decimal numbers. J Math Stat 4:15

Al-Saidi NMG, Said MRM (2009) A new approach in cryptographic systems using fractal image coding. J Math Stat 5:183

Al-Saidi NMG, Said MRM (2014) Biometric identification using local iterated function. Eur Phys J Spec Top 1–16

Al-Saidi NMG, Said MRM, Ahmed AM (2011) Efficiency analysis for public key systems based on fractal functions. J Comput Sci 7:526

Cavoukian A, Stoianov A (2011) Biometric encryption. Encyclopedia of cryptography and security. Springer, US, pp 90–98

Dang PP, Chau PM (2000) Image encryption for secure internet multimedia applications. IEEE Trans Consum Electron 46:395–403

Das AK (2011) Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. Inf Secur IET 5:145–151

Dhawan S (2011) A review of image compression and comparison of its algorithms. Int J Electron Commun Technol 2(1)

Gaddam SVK, Lal M (2010) Efficient cancelable biometric key generation scheme for cryptography. IJ Netw Secur 11:61–69

Jain AK, Karthik N (2012) Biometric Authentication: system security and user privacy. IEEE Comput 45:87–92

Jain AK, Arun AR, Karthik N (2011) Introduction to biometrics. Springer, Germany

Kaur M, Sofat S, Deepak S (2010) Template and database security in Biometrics systems: a challenging task. Int J Comput Appl 4:1–5

Khan MK, Zhang J, Tian L (2005) Protecting biometric data for personal identification. Advances in biometric person authentication. Springer, Berlin, Heidelberg, pp 629–638

Khan MK, Xie L, Zhang J (2007) Robust hiding of fingerprint-biometric data into audio signals. Advances in biometrics. Springer, Berlin, Heidelberg, pp 702–712

Liu Y, Sun J-G (2010) Face recognition method based on FLPP. In: Electronic commerce and security (ISECS), 3rd international symposium on, IEEE

Rahman S (2010) Curvelet texture based face recognition using principal component analysis. In: Computer and information technology (ICCIT), 13th international conference on. IEEE

Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM syst J 40:614–634

Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 1–25

Sabena F, Dehghantanha A, Seddon AP (2010) A review of vulnerabilities in identity management using biometrics. In: Future Networks, ICFN'10. 2nd international conference on IEEE

Shakhnarovich G, Moghaddam B (2011) Face recognition in subspaces. Handbook of face recognition. Springer London, pp 19–49

Xi K (2011) A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. Secur Commun Netw 4:487–499