International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

Improvement of Digital Data Security by The Application of Elliptic Curve Cryptography and Butterfly Genetic Algorithm

Kartikey Pandey[1], *Deepmala Sharma*[2]
[1]*Research Scholar, Department of Mathematics, National Institute of Technology, Raipur, Chhattisgarh, India.*
[2]*Associate Professor, Department of Mathematics, National Institute of Technology, Raipur, Chhattisgarh, India.*
Email ID: *nitiankartik@gmail.com*[1], *deepsha.maths@nitrr.ac.in*[2]

Abstract
Digital advancements have significantly increased comfort in various technical and non-technical fields. In this era, digital images are widely used in authentication systems, making the security of such images a critical concern. This paper proposes an innovative image security model that focuses on protecting an embedded secret signature in the low-frequency regions of digital images. The model employs Elliptic Curve Cryptography (ECC) for strong encryption and uses the Butterfly Genetic Algorithm (BGA) to enhance security by optimizing the embedding process. The use of the BGA improves robustness against spatial attacks by efficiently shuffling and embedding the image data. Experimentation on a standard image dataset demonstrates that the proposed model achieves superior PSNR and SNR values when compared to existing image security techniques, thereby enhancing both image quality and security.
Keywords: *Image Encryption, Data Security, Elliptic Curve Cryptography, Butterfly Genetic Algorithm*

1. Introduction
At present, the rapid growth in popularity of images can be witnessed in a number of fields ranging from medical imaging and surveillance to biometric authentication and multimedia communications. Therefore, with the increases in the use of images comes an increase in the need to protect them from miscues and illegal access, especially when they carry sensitive information. Without proper restrictions in place, image distortion and copy would result to invading privacy, stealing identity and data breach. Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) have become commonplace to protect images (Al-Gindy (2009), Hanayong (2021), Rijmen (2001), Standard (1999)). Digital images secured with any of the encryption methods mentioned above are also effective; however, the application of these algorithms typically comes with per hysterical penalties which result in reduction of picture quality creating a breach in real time, resource limited environment. Furthermore, these methods have their shortcomings pertaining sophisticated attacks, especially those which target the image spatial domain. This has resulted in an increasing demand for image encryption techniques that provide high security and are computationally efficient while maintaining image quality. One such promising solution for digital image encryption is ECC (Benssalah (2021), Kumar (2024), Parida (2021)). ECC offers significant encryption while having much smaller key sizes compared to traditional methods. This reduces the computational complexity involved but maintains the security. Cryptography is alone not capable of protecting the images in spatial domain attacks, where an attacker varies pixel values to obtain covered information or modify the image. To this end, optimization techniques have been explored, including Genetic Algorithms. Among these, the Butterfly Genetic Algorithm proved highly effective because of its improved shuffling and search ability; hence, it ideally suited for optimizing the embedding of hidden information into images. Motivated by a need for improvement in image security both in cryptographic strength and in security against attack, this work aims to develop an innovative image security model based on the integration of ECC and BGA. Therefore, this research work is aimed at achieving a secure, efficient, and high-quality encryption solution that

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

not only safeguards the image but also keeps the video as visually faithful as possible. The proposed model focuses on embedding a secret signature in the low-frequency regions of the image, since these have the least influence of common image processing operations such as compression and filtering. Furthermore, the model makes use of ECC for encryption and BGA for optimizing the embedding process so as to ensure that there is security guaranteed on the image but at the minimum risk of quality degradation. The novelty of this research lies in the introduction of a new approach which integrates ECC with BGA to ensure image security, embedding a low-frequency region so that the quality of the image would remain protected, and improving PSNR and SNR values compared to other image encryption techniques. In this regard, the model shows increased resistance towards spatial domain attacks as the BGA shuffles and obfuscates the data of images effectively. In summary, this research delivers an all-round solution to improve the security of digital images in the sense that the strength of encryption, efficiency, and maintaining the quality are balanced and cater to the emerging trend of safe image transfer and storage in the modern digital environment.

2. Related Work

A great research area has been driven by the need to protect such sensitive data in imaging applications, including medical imaging, surveillance, and biometric authentication. Traditional encryption methods, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) (Hanayong (2021), Muhammad (2014), Rijmen (2001), Selent (2010)), are widely used but suffering, therefore, from high computational costs due to large numbers of operations and a probable degradation in image quality. These methods become less efficient when dealing with large images or in real-time, resource-constrained environments, such as IoT and mobile devices. They provide robust security; however, their optimization towards visual data is not achieved. To overcome the limitations of traditional cryptography, chaotic systems have been introduced. Chaotic maps such as the Logistic Map, Lorenz System, and Chen's Chaotic System are effective for confusion and diffusion processes in image encryption (Cedillo-Hernandez (2015), Chang (2020), Daoui (2022), Vaishnavi (2015), Zhou (2017)). Although they offer lightweight and fast encryption, chaotic maps can be vulnerable if their parameters are known, and they struggle against spatial domain attacks that manipulate pixel values.

ECC provides strong security through small key sizes, thus enabling efficient computation for image encryption (Benssalah (2021), Kumar (2024), Parida (2021), Singh (2022)). Studies show that ECC-based image encryption systems can surpass RSA systems, mainly in terms of speed and key management; hence they are suitable for low-power devices with secure image transmission. However, ECC is not the safeguard against manipulation attacks and requires further optimizations. Genetic Algorithms (GAs) have been used in optimizing encryption processes, especially in embedding secret data, such as digital watermarks or signatures. GAs enhances the robustness of pixel-shuffling processes, therefore making it difficult for attackers to extract or modify hidden data (Al-Husainy (2006), Arora (2019), Cedillo-Hernandez (2015), Chang (2020), Vaishnavi (2015), Zhou (2017)). However, traditional GAs suffer from drawbacks, such as slow convergence, which greatly restrict their use. This has led to the development of sophisticated GAs, like the Butterfly Genetic Algorithm (BGA), offering superior optimization by avoiding local optima and increasing randomness in the encrypted data. However, combining ECC with GAs, especially BGA, has been believed to enhance the security in images (Al-Husainy (2006), Al-Gindy (2009), Arora (2019), Chen (2017), Selent (2010), Singh (2022), Zhou (2021)). Latest literature focused on hybrid methods in which ECC acts as the cryptographic base and GAs optimize the embedding process by ensuring better security as well as quality in images. Even with this development, the potential of using advanced genetic algorithms like BGA with ECC for the effective encryption of images has not been exhausted in full.

In conclusion, although ECC and GAs have enhanced image security individually, the potential of their integration remains unexplored in the direction of hybrid combinations, especially with optimization

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

algorithms such as BGA. This paper aims to fill this gap by integrating ECC and BGA and enhancing the quality of enciphered images along with their security, thus overcoming some of the shortcomings present in computational efficiency and resistance against attacks. This section provides a thorough description of an image encryption model under proposal, integrating ECC with the butterfly genetic algorithm to improve security in images. The model is designed so as to optimize the encryption process while maintaining high security together with quality preservation during encryption of the image. This model comprises three major phases: encryption with the help of ECC, embedding using BGA, and decryption. In this section, we define each component of the model together with mathematical formulation of the involved processes.

2.1.Phase 1: Elliptic Curve Cryptography (ECC) for Image Encryption

Elliptic Curve Cryptography (ECC) is employed in the proposed model to provide a secure method for encrypting the secret signature to be embedded into the image. ECC operates over the algebraic structure of elliptic curves, making it both computationally efficient and secure.

2.1.1. Elliptic Curve Equation

The elliptic curve used in ECC is defined over a finite field F_p (a prime field) and is given by the equation:

$$y^2 = x^3 + ax + b$$

where p is a prime number, a and b are constants that define the shape of the elliptic curve? The points on the curve, along with a point at infinity, form an abelian group, which is the basis for ECC.

2.1.2. Key Generation in ECC

- **Private Key:** A random integer d_A is chosen as the private key, where $1 < d_A < n - 1$, and n is the order of the elliptic curve.
- **Public Key:** The corresponding public key is generated as: $P_A = d_A \times G$ where G is a generator point on the elliptic curve, and $\times$ denotes scalar multiplication.

2.1.3. Encryption with ECC

Let the message (the secret signature) be represented by a point M on the elliptic curve. The encryption process in ECC involves two steps:

- Choose a random integer k where $1 < k < n - 1$.
- Generate the ciphertext consisting of two points C_1 and C_2: $C_1 = k \times G$, $C_2 = M + k \times P_B$, where P_B, where P_B is the public key of the recipient.
- The pair (C_2, C_2) is the encrypted message (signature).

2.1.4. Decryption with ECC

To decrypt the ciphertext (C_2, C_2), the recipient uses their private key d_B as follows:

$$M = C_2 - d_B \times C_1$$

This retrieves the original message M, which represents the secret signature to be embedded into the image.

2.2.Phase 2: Butterfly Genetic Algorithm (BGA) for Embedding Optimization

Once the secret signature is encrypted using ECC, it is embedded into the image using the Butterfly Genetic Algorithm (BGA). The BGA optimizes the embedding process by ensuring the encrypted signature is hidden in the low-frequency regions of the image, thereby preserving image quality and enhancing robustness against attacks.

2.2.1. Representation of the Image

The input image is represented as a two-dimensional matrix I of pixel values, where each pixel is denoted by $I(i,j)$. The goal is to embed the encrypted signature into the low-frequency regions of the image. These regions are identified using frequency domain transformations, such as the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), which separate the image into frequency components.

2.2.2. Embedding Process

- **Apply DCT/DWT:** The image matrix I is transformed into the frequency domain using DCT or DWT:

  $$F = T(I)$$

  Where T represents the chosen transformation (DCT or DWT), and F is the frequency-domain representation of the image.
- **Low-Frequency Region Selection:** The low-frequency components of F are selected, as they are less sensitive to image processing operations like compression.
- **Embedding the Encrypted Signature:** The

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

encrypted signature (C_2, C_2), is embedded into the low-frequency components of the image. The embedding process is optimized using BGA, which shuffles and adjusts the coefficients to minimize the distortion introduced by embedding.

2.2.3. Butterfly Genetic Algorithm (BGA)

The Butterfly Genetic Algorithm improves the embedding process by optimizing the position and distribution of the encrypted data within the low-frequency region. The BGA mimics the foraging behavior of butterflies and is designed to avoid local optima in the search space, ensuring a global solution is found for optimal embedding.

The main steps of BGA are:

- **Initialization:** Generate an initial population of possible embedding solutions, each representing a different way to embed the encrypted signature into the image.
- **Fitness Function:** The fitness of each solution is evaluated based on its impact on the Peak Signal-to-Noise Ratio (PSNR) and Signal-to-Noise Ratio (SNR), which measure image quality preservation. The fitness function is given by:

$$Fitness = \alpha.PSNR + \beta.SNR$$

  Where α and β are weights that balance the importance of PSNR and SNR.
- **Selection and Crossover:** The best solutions are selected based on their fitness, and new solutions are generated using crossover, where two "parent" solutions combine to produce a "child" solution that inherits characteristics from both parents.
- **Mutation:** A mutation operation is applied to introduce randomness into the solutions, enhancing the algorithm's ability to explore the search space.
- **Convergence:** The process repeats until the algorithm converges to an optimal embedding solution.

2.3.Phase 3: Decryption and Recovery

To recover the original image and the embedded secret signature, the decryption process consists of the following steps:

- **Extract the Encrypted Signature:** The embedded encrypted signature (C_2, C_2) is extracted from the low-frequency region of the image using the inverse of the embedding process.
- **Decrypt the Signature:** Using ECC decryption, the original signature M is recovered:

$$M = C_2 - d_B \times C_1$$

- **Reconstruct the Image:** The image is reconstructed by applying the inverse DCT or DWT to the modified frequency components:

$$I' = T^{-1}(F')$$

where F' is the frequency-domain representation of the image with the signature embedded, and I' is the recovered image.

3. Experimental Results and Analysis

This section discusses the experimental results of the proposed image encryption model based on Elliptic Curve Cryptography (ECC) and the Butterfly Genetic Algorithm (BGA). The analysis demonstrates the performance of the model by judging its quality in terms of PSNR, SNR, SSIM, and its ability to prevent common attacks. In addition, the computational efficiency aspect is analyzed to determine the suitability of this model in real-time applications.

3.1.Experimental Setup

The model was implemented in Python and MATLAB using standard libraries for image processing and cryptographic functions. A variety of standard grayscale and color images from a public dataset (e.g., Lena, Baboon, and Peppers) were used to evaluate the model's robustness and consistency across different image types. The images varied in size and detail complexity to assess performance across different scenarios. Experiments were conducted on a system equipped with an Intel Core i7 processor and 16 GB RAM, with the BGA parameters optimized for effective embedding while minimizing image distortion.

3.2.Performance Metrics

The following metrics were used to evaluate the model:

- **Peak Signal-to-Noise Ratio (PSNR):** Measures the difference between the original and encrypted images; higher values indicate better image quality retention.

$$PSNR = 10.log_{10}(\frac{MAX_I^2}{MSE})$$

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

- Where MAX_I is the maximum pixel value (255 for an 8-bit image), and MSE (Mean Squared Error) is the average squared difference between the original and encrypted image.

- **Signal-to-Noise Ratio (SNR):** Provides a comparative measure of signal power to the noise introduced during encryption.

$$SNR = 10.log_{10}(\frac{\sum_{i,j} I(i,j)^2}{\sum_{i,j}(I(i,j) - I'(i,j))^2})$$

- **Structural Similarity Index Measure (SSIM):** Assesses structural similarity to the original image, capturing distortions in luminance, contrast, and structure.
- **Encryption and Decryption Time:** Time taken for encryption and decryption was recorded to evaluate the computational efficiency of the model.

3.3.Image Quality Analysis

3.3.1. PSNR and SNR Results

The PSNR and SNR values of the encrypted images for different test images demonstrate the model's ability to maintain image quality. Higher PSNR and SNR values indicate that the encrypted images retain high fidelity to the original images.

Table 1 PSNR, SNR and SSIM Results

IMAGE	PSNR (dB)	SNR (dB)	SSIM
Lena	48.32	45.76	0.97
Baboon	44.15	42.67	0.95
Peppers	46.89	44.35	0.96

Results in Table 1 demonstrate that the BGA successfully embeds encrypted data without remarkable degradation of image quality. Lena gets the highest PSNR because of smoothness in texture, whereas Baboon having very high texture depicts relatively low PSNR because images are very sensitive to noise.

3.3.2. SSIM Results

SSIM values for each test image were above 0.95, indicating minimal structural distortion: These high SSIM values from Table 1 indicate that the encrypted images closely preserve structural details of the original, demonstrating the robustness of the BGA in retaining perceptual quality.

3.4.Robustness Against Attacks

The model's robustness was evaluated by subjecting the encrypted images to common attacks, including noise addition, image cropping, and JPEG compression.

3.4.1. Noise Attack

Gaussian noise was added to the encrypted images at different levels (variance of 0.01, 0.02, 0.05) to test robustness. Despite noise addition, the model retained high PSNR and SSIM values:

Table 2 Noise Attack Analysis

IMAGE	Noise Variance	PSNR after attack (dB)	SSIM after attack
Lena	0.01	42.10	0.92
Lena	0.02	39.57	0.89
Lena	0.05	37.22	0.85

The high SSIM and PSNR values shown in Table 2 indicate that the model's embedding strategy, focused on low-frequency regions, improves resistance to noise.

3.4.2. Image Cropping Attack

Partial image cropping was performed to evaluate robustness. The encrypted signature remained largely recoverable even after cropping up to 25\% of the image: Image Crop Percentage PSNR after Attack (dB) SSIM after Attack.

Table 3 Cropping Attack Analysis

IMAGE	PSNR (dB)	PSNR after attack (dB)	SSIM after attack
Lena	10%	43.85	0.91
Lena	25%	41.27	0.88

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

This resilience against cropping can be attributed to the strategic placement of embedded data, optimized through BGA to maintain integrity in accessible regions.

3.4.3. JPEG Compression

The model's resistance to JPEG compression was assessed by compressing encrypted images at various quality levels. The results below show the resilience of the model to typical compression rates:

Table 3 JPEG Compression

IMAGE	PSNR (dB)	SNR (dB)	SSIM
Lena	90%	45.32	0.94
Lena	70%	41.88	0.91
Lena	50%	38.23	0.86

These values indicate that embedding in low-frequency regions, which are less affected by JPEG compression, maintains image quality under compression.

3.5.Comparative Analysis

The ECC-BGA model was compared with traditional encryption methods, AES and RSA, focusing on encryption time and image quality retention:

Table 3 PSNR, SNR and SSIM Results

IMAGE	Model	Encryption time	PSNR (dB)
Lena	48.32	0.89	48.32
	44.15	1.24	46.75
	46.89	2.05	43.56

The ECC-BGA model achieves higher PSNR and lower encryption times than both AES and RSA, illustrating its efficiency and quality retention.

Conclusion

The proposed image encryption model combines Elliptic Curve Cryptography with Butterfly Genetic Algorithm. The combination introduces a strong solution for securing digital images. ECC uses smaller key sizes to deliver the best possible cryptographic security while making it efficient for application in resource-constrained environments. The BGA optimizes the embedding of encrypted data into low-frequency regions of images. With this integration, security and image quality both benefit highly, as experimental evaluation values in PSNR and SNR are highly improved. One of the main advantages of this model is its high security achieved through ECC, which offers comparable protection to traditional methods like RSA but with reduced computational demands. Additionally, the optimization provided by the BGA ensures that the embedding process minimizes visual distortions, thereby maintaining high image quality. The model's efficiency makes it suitable for applications requiring a balance between security and performance, especially in mobile and IoT contexts. However, the model also has some disadvantages. The complexity introduced by the BGA can lead to longer processing times, which may not be suitable for applications that require rapid encryption. Moreover, while the BGA improves optimization, it may still encounter local optima, impacting performance if not properly tuned. Robustness of the model-the model may not be robust against advanced attacks like differential or side-channel attacks. Frequency domain techniques, such as DCT and DWT dependence, could restrict its applicability to specific formats of images and result in suboptimal performance under certain conditions. Overall, though ECC-BGA hybrid model can overcome serious challenges in image encryption, its real-time applicability may be enhanced and made more resilient against a wider range of attacks in the future research.

References

[1]. Al-Husainy, M. A. (2006). Image encryption using genetic algorithm. Information Technology Journal, 5(3), 516-519.
[2]. Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., \& Tawfik, A. (2009, December). A high

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

capacity digital watermarking technique for the authentication of colour images. In 2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT) (pp. 37-42). IEEE.

[3]. Arora, S., & Singh, S. (2019). Butterfly optimization algorithm: a novel approach for global optimization. Soft computing, 23, 715-734.

[4]. Benssalah, M., Rhaskali, Y., & Drouiche, K. (2021). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. Multimedia Tools and Applications, 80(2), 2081-2107.

[5]. Cedillo-Hernandez, M., Garcia-Ugalde, F., Nakano-Miyatake, M., \& Perez-Meana, H. (2015). Robust watermarking method in DFT domain for effective management of medical imaging. Signal, Image and Video Processing, 9, 1163-1178.

[6]. Chang, C. C., Chen, J. Y., Chen, Y. H., \& Liu, Y. (2020). A Reversible Data Hiding Method for SMVQ Indices Based on Improved Locally Adaptive Coding. Int. J. Netw. Secur., 22(4), 575-583.

[7]. Chen, W. H., Zhou, X. F., Li, M. J., \& Hu, M. (2023). Image encryption algorithm based on optical chaos and elliptic curve. The European Physical Journal D, 77(11), 1-18.

[8]. Daoui, A., Yamni, M., Karmouni, H., Sayyouri, M., Qjidaa, H., Ahmad, M., \& Abd El-Latif, A. A. (2022). Biomedical Multimedia encryption by fractional-order Meixner polynomials map and quaternion fractional-order Meixner moments. IEEE Access, 10, 102599-102617.

[9]. Devi, B. P., Singh, K. M., \& Roy, S. (2016). A copyright protection scheme for digital images based on shuffled singular value decomposition and visual cryptography. SpringerPlus, 5, 1-22.

[10]. Hanayong, J., Zarlis, M., \& Sihombing, P. (2021, June). Implementation of image security using elliptic curve cryptography RSA algorithm and least significant bit algorithm. In Journal of Physics: Conference Series (Vol. 1898, No. 1, p. 012016). IOP Publishing.

[11]. Kumar, S., \& Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artificial Intelligence Review, 57(4), 87.

[12]. Li, J., \& Miao, S. (2013, March). The Medical Image Watermarking Using Arnold Scrambling and DFT. In Conference of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013) (pp. 192-195). Atlantis Press.

[13]. Muhammad, S. J., Chiroma, H., \& Mahmud, M. (2014). Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: issues and challenges. J Theor Appl Inf Technol, 61(1), 2349.

[14]. Parida, P., Pradhan, C., Gao, X. Z., Roy, D. S., \& Barik, R. K. (2021). Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. IEEE Access, 9, 76191-76204.

[15]. Rijmen, V., \& Daemen, J. (2001). Advanced encryption standard. Proceedings of federal information processing standards publications, national institute of standards and technology, 19, 22.

[16]. Selent, D. (2010). Advanced encryption standard. Rivier Academic Journal, 6(2), 1-14.

[17]. Singh, P., Devi, K. J., Thakkar, H. K., \& Kotecha, K. (2022). Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. IEEE Access, 10, 8974-8993.

[18]. Standard, D. E. (1999). Data encryption standard. Federal Information Processing Standards Publication, 112, 3.

[19]. Vaishnavi, D., \& Subashini, T. S. (2015). Robust and invisible image watermarking in RGB color space using SVD. Procedia Computer Science, 46, 1770-1777.

[20]. Zhou, H., Cheng, H. Y., Wei, Z. L., Zhao, X., Tang, A. D., \& Xie, L. (2021). A hybrid butterfly optimization algorithm for

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.503
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3419-3426

numerical optimization problems. Computational Intelligence and Neuroscience, 2021(1), 7981670.

[21]. Zhou, Z., Chen, S., \& Wang, G. (2017). A robust digital image watermarking algorithm based on dct domain for copyright protection. In Smart Graphics: 13th International Symposium, SG 2015, Chengdu, China, August 26-28, 2015, Revised Selected Papers 13 (pp. 132-142). Springer International Publishing.