

SISTEM PRESENSI ANDROID BERBASIS QR CODE DAN DSRSA MENGUNAKAN *TEMPLATE MATCHING*

Cahya Rahmad¹, Dika Rizky Yunianto², Bayu Hari Saputro³, Dimas Rossiawan H.P⁴

^{1,2,3}Jurusan Teknologi Informasi, Politeknik Negeri Malang

⁴Jurusan Teknik Elektro, Politeknik Negeri Malang

¹cahya.rahmad@polinema.ac.id, ²dikarizkyunianto@polinema.ac.id, ³bayuhari@polinema.ac.id,

⁴dimas.rossi@polinema.ac.id

Abstrak

Pelaksanaan sistem presensi pada Jurusan Teknologi Informasi di Politeknik Negeri Malang perlu dikembangkan agar lebih efektif dalam implementasinya. Efektifitas yang dimaksud adalah mahasiswa tidak perlu lagi untuk mengambil lembar presensi saat akan melakukan presensi perkuliahan dan mengembalikan lembar tersebut setelah selesai melakukan presensi. Penelitian ini bertujuan untuk membangun suatu sistem presensi untuk menjawab permasalahan yang telah dipaparkan. Dalam pembangunan sistem presensi, digunakan 2 algoritma yaitu *DS RSA* dan *Template Matching*. Algoritma *DS RSA* yang disisipkan pada pembangkitan *QR Code* digunakan demi keamanan dan reliabilitas pada pengacakan kunci yang telah diinisialisasi oleh algoritma *DS RSA*. Pengacakan itu bermaksud untuk memberikan batasan pada mahasiswa agar tidak bisa melakukan presensi jika kelasnya tidak sesuai. Sedangkan untuk *Template Matching* digunakan untuk pengecekan wajah mahasiswa. Hal ini dilakukan untuk memastikan bahwa mahasiswa tersebut hadir pada kelas dan dosen dapat mengantisipasi adanya kecurangan mahasiswa dalam melakukan absensi. Penerapan sistem presensi ini membutuhkan setiap mahasiswa untuk memfoto wajah mereka lalu membaca *QR Code* yang telah dibangkitkan dengan *smartphone* sesuai dengan kelas dan ditampilkan pada layar proyektor kelas. Penelitian ini berhasil membangun sistem presensi berbasis *QR Code* dengan mengimplementasikan algoritma *DS RSA* dan *template matching*. Sistem pembangkitan *QR Code* ini memiliki reliabilitas sangat baik dan akurasi tertinggi dari algoritma *template matching* adalah 93.33% dengan jumlah 80 *template*.

Kata kunci : *Digital Signature RSA, Deteksi Wajah, QR Code, Sistem Absensi, Template Matching.*

1. Pendahuluan

Selama ini sistem presensi institusi pendidikan tinggi di Indonesia masih didominasi oleh sistem yang konvensional, salah satu contohnya adalah pada Politeknik Negeri Malang khususnya pada jurusan Teknologi Informasi. Dalam eksekusinya di jurusan Teknologi Informasi Politeknik Negeri Malang, sebelum dosen melakukan presensi di kelas, mahasiswa diharuskan mengambil kertas presensi di admin terlebih dahulu, lalu mengembalikannya ke admin setelah perkuliahan selesai. Dari paparan penjelasan alur sistem konvensional tersebut, penulis menyadari adanya permasalahan mobilisasi dimana kadang tempat pengambilan kertas presensi tidak satu gedung dengan tempat perkuliahan.

Perkembangan teknologi saat ini dapat dijadikan sebagai solusi untuk mengatasi permasalahan tersebut salah satunya adalah memadukan teknologi *Quick Response Code (QR Code)* dengan *Digital Signature RSA* dan *Face Detection* untuk pembangunan sistem absensi di jurusan Teknologi Informasi Politeknik Negeri Malang. *QR code* adalah sebuah kode matriks 2 (*private* dan *public*) dimensi yang dibuat oleh perusahaan Jepang Denso-Wave pada tahun 1994

(Rochman, Raharjana and Taufik, 2017). Kriptografi asimetris adalah sebuah algoritma yang kriptografi yang menggunakan 2 kunci yang berbeda untuk melakukan enkripsi dan dekripsi (Kittur and Pais, 2017),(Ani *et al.*, 2011). Metode *template matching* juga handal untuk *face detection* (Çinar Akakin *et al.*, 2006),(Wijanarko *et al.*, 2017).

Oleh karena itu, diusulkan sebuah sistem presensi *QR Code* yang dipadukan dengan *digital signature RSA* dan *face detection* menggunakan metode *Template Matching* berbasis Android. Alur sistem tersebut adalah dosen akan *generate QR Code* yang sudah di enkripsi menggunakan kunci *private* dan hasilnya akan ditampilkan di depan kelas, lalu mahasiswa hanya perlu *scanning QR code* melalui *smartphone* untuk melakukan presensi. Penggunaan algoritma enkripsi pada sistem pengacakan *QR Code* didasari oleh keamanan, reliabilitas dan untuk memberikan otoritas kepada mahasiswa yang sesuai dengan kelas masing-masing. Sebelum melakukan presensi mahasiswa harus memfoto wajah terlebih dahulu, hasil dari foto tersebut akan dicek menggunakan *face detection* dengan metode *template matching* dan *normalized cross correlation* untuk mengetahui apakah gambar sudah memenuhi syarat atau belum, jika gambar sudah memenuhi syarat maka

gambar akan ditampilkan diproyektor jika berhasil presensi untuk menghindari kecurangan titip presensi. Setiap beberapa satuan waktu tertentu maka QR code akan otomatis berubah untuk menghindari kecurangan mahasiswa untuk melakukan presensi tanpa adanya kehadiran di kelas. Jika mahasiswa sudah berhasil melakukan presensi maka datanya akan otomatis tersimpan oleh sistem. Dengan adanya sistem ini maka diharapkan dapat memangkas proses mobilisasi sistem presensi menjadi lebih lebih efektif.

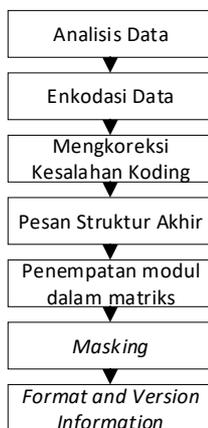
2. Landasan Teori

2.1 QR Code

QR Code (*Quick Response Code*) merupakan sebuah matriks 2 dimensi yang dapat menyimpan data berupa tulisan, gambar, dan sebagainya. Dikembangkan oleh Denso Corporation Jepang untuk perusahaan otomotif pada tahun 1994. Contoh QR Code dapat dilihat pada Gambar 1 (Dudheria, 2018). Dalam QR Code terdapat 2 prosedur yaitu pembangkitan QR (*Generate*) dan pembacaan QR Code (*Scanning*). Prosedur pembangkitan QR Code dapat dilihat pada Gambar 2. Prosedur pembacaan QR Code adalah proses sebaliknya dari pembangkitan QR Code, dapat dilihat pada gambar 3 (Ani *et al.*, 2011), (Dudheria, 2018).



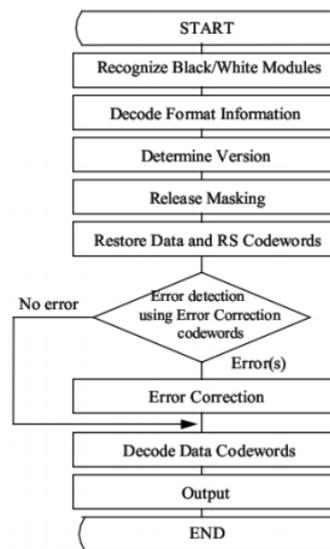
Gambar 1. Contoh QR Code



Gambar 2. Diagram Pembangkitan QR Code

QR Code, yaitu mengkodekan serangkaian teks. Terdapat empat mode untuk menyandikan teks yaitu numerik, alfanumerik, *byte*, dan kanji. Setiap mode mengkodekan teks sebagai *string* bit (1s dan 0s). Analisis data memiliki tujuan untuk menentukan

apakah teks dapat dikodekan dalam mode numerik, alfanumerik, *byte*, atau kanji, lalu memilih mode yang paling optimal. Setelah memilih mode penyandian yang sesuai, langkah selanjutnya adalah enkodasi data atau menyandikan data. Proses ini menghasilkan serangkaian bit yang dipecah menjadi data yang masing-masing berukuran 8 bit. QR Code menggunakan koreksi kesalahan, setelah membuat *string* bit data yang mewakili teks yaitu *Reed-Solomon*. Pemindai QR membaca kata sandi data dan kata sandi koreksi kesalahan kemudian membandingkan keduanya, pemindai dapat menentukan apakah proses membaca data sudah berjalan dengan benar, pemindai ini juga dapat memperbaiki kesalahan jika tidak membaca data dengan benar. Bagian pengkodean koreksi kesalahan menjelaskan proses menghasilkan kata sandi koreksi kesalahan secara terperinci



Gambar 3. Diagram Pembacaan QR Code

2.2 Digital Signature

Digital Signature adalah suatu konsep untuk memastikan dokumen digital tetap terjaga keaslian dan keamanannya (Kittur and Pais, 2017). Pertama kali diperkenalkan oleh perusahaan adobe pada tahun 1999, pertama diterapkan pada file PDF dan sekarang penggunaan *Digital Signature* sendiri sudah berkembang bukan hanya untuk dokumen namun juga dapat digunakan sebagai keamanan transaksi dan *login*. Pesan Struktur akhir mengatur *codeword* koreksi data dan kesalahan pada langkah sebelumnya sehingga berisi urutan yang tepat. Setelah membuat kata sandi data dan kata sandi koreksi kesalahan dan mengaturnya dalam urutan yang benar, penempatan bit dalam matriks QR code pada *codeword* disusun dalam matriks seperti cara tertentu, seperti kotak di tiga sudut. Pola tertentu dalam matriks QR Code dapat mempersulit pemindai untuk membaca kode dengan benar. Untuk mengatasi hal ini, spesifikasi QR Code mendefinisikan delapan pola pada *masking*, yang

masing-masing mengubah kode QR sesuai dengan pola tertentu dan mengevaluasi lalu menggunakan pola *masking* yang menghasilkan skor pinalti terendah. Langkah terakhir adalah menambahkan format dan jika perlu informasi versi ke *QR code* dengan menambahkan piksel di area tertentu dari kode yang dibiarkan kosong pada langkah sebelumnya. Piksel format mengidentifikasi tingkat koreksi kesalahan dan pola *masking* yang digunakan dalam *QR code* ini. Piksel versi menyandikan ukuran matriks QR dan hanya digunakan dalam *QR code* yang lebih besar.

2.3 RSA

RSA diperkenalkan oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1977 (Dudheria, 2018). RSA diketahui sebagai algoritma pertama yang paling cocok untuk proses signing dan encryption dan merupakan jenis kriptografi kunci publik (memiliki 2 kunci privat dan publik). RSA masih sangat diimplementasikan secara luas terutama dibidang transaksi karena dipercaya sangat aman dengan kunci yang cukup panjang (Bao, Lee and Hwang, 2006), (Arifin *et al.*, 2009). Penerapan skema RSA pada *Digital Signature* adalah:

1. Memilih 2 bilangan prima p dan q dengan syarat:

$$P! = q \tag{1}$$
2. Menghitung n dengan Persamaan 2:

$$n = p \times q \tag{2}$$
3. Menghitung φ(n) dengan Persamaan 3:

$$\varphi(n) = (p - 1)(q - 1) \tag{3}$$
4. Memilih kunci publik e yang relatif prima dengan φ(n)
5. Menghitung d dengan Persamaan 4:

$$d = 1 + (k \times \varphi(n)) / e, 0 < k < \infty$$

$$\text{dan } 1 + (k \times \varphi(n)) \bmod e = 0 \tag{4}$$
6. Akan didapat pasangan kunci publik (e, n) dan pasangan kunci privat (d, n).

Setelah kunci privat dan publik sudah ditentukan, maka proses ini bisa dilakukan. Langkah-langkahnya adalah:

1. Menkonversi input string (*message*) menjadi hash values dengan algoritma SHA-1.
2. Mengkonversi hasil hash message menjadi angka ASCII
3. Proses Enkripsi dilakukan dengan Persamaan 5:

$$C = H^e \bmod \tag{5}$$

C = ciphertext
 H = hash plaintext
4. Setelah dienkripsi selanjutnya adalah pembuatan *signed document* yang isinya *ciphertext* dan *hash plaintext*.
5. Selanjutnya adalah proses Dekripsi, proses ini dilakukan dengan Persamaan 6:

$$C = H^d \bmod \tag{6}$$

C = ciphertext
 H = hash plaintext

Terakhir adalah pencocokan, jika H = hash *plaintext* dari *signed document* maka dokumen telah terverifikasi.

2.4 Template Matching

Template Matching adalah sebuah teknik dalam pengolahan citra digital untuk menemukan bagian-bagian kecil dari gambar yang cocok dengan *template* gambar. Memang bagi penglihatan kita, sangatlah mudah untuk mengidentifikasi objek pada suatu citra terutama wajah, namun bagi komputer itu akan menjadi pekerjaan yang sangatlah susah, oleh karena itu metode *Template Matching* merupakan salah satu metode yang dapat digunakan menjawab masalah tersebut (Trivedi, Thounaojam and Pal, 2018), (Thakar *et al.*, 2017) (Jin *et al.*, 2007).

Dalam kasus ini digunakan pencocokan antara image gambar (foto) dengan template wajah yang sudah disediakan. Untuk mengetahui prosentase tingkat kemiripan template dengan berkas citra wajah digunakan perhitungan NC (*Normalized Cross Corelation*) [7]. Nilai NC diperoleh dengan membandingkan *template* dengan berkas wajah. Semakin prosentase nilai NC mendekati 100 %, maka perbandingan template dengan berkas citra wajah semakin cocok. Untuk menentukan nilai NC digunakan Persamaan 7 berikut:

$$NC = \frac{\sum_i \sum_j w_{ij} w'_{ij}}{\sqrt{\sum_i \sum_j |w_{ij}|^2}} \tag{7}$$

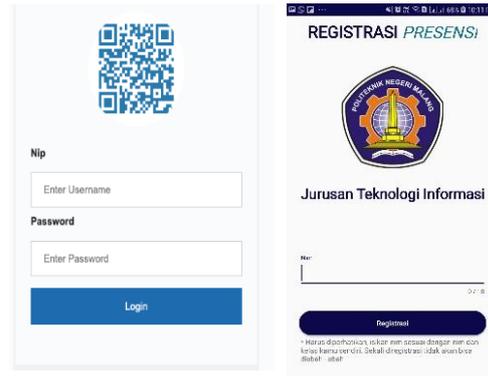
3. Metodologi

Implementasi sistem mengacu pada perancangan aplikasi. Implementasi sistem dilakukan dengan menggunakan bahasa PHP dengan *framework* Laravel yang dipadukan dengan rest api volley untuk *server* dan *website* disisi dosen, lalu java android mobile disisi mahasiswa. Dosen menampilkan *QR Code* melalui layer proyektor dan mahasiswa memindai *QR Code* melalui smartphone mereka masing-masing seperti pada Gambar 10. Bagi yang tidak memiliki HP atau tertinggal, sistem absensi ini menyediakan absensi secara manual untuk permasalahan tersebut. *Database* yang digunakan adalah MySql. Implementasi sistem meliputi: pembuatan *interface* aplikasi disisi *website* dan *mobile*. Dilanjutkan dengan pembuatan *database* dan memasukkan data - data yang diperlukan seperti absensi dan data dosen. Langkah ketiga yaitu menerapkan metode DS RSA untuk pengacakan *QR Code*, pembentukan *QR Code* dan pembacaan *QR Code* dan langkah terakhir adalah Menerapkan metode *Template Matching* untuk pengecekan wajah. *Activity diagram* sistem dapat dilihat pada Gambar 4 dibawah ini.

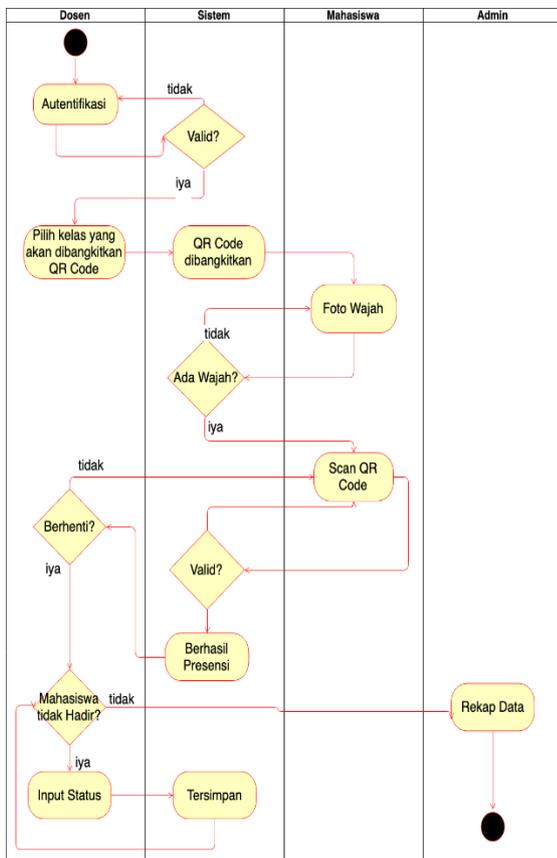
4. Implementasi dan Hasil

Hasil implementasi dari desain antar muka dapat dilihat pada Gambar 5, 6, 7, dan 8. Dari 15 sampel yang diambil dengan kriteria *smartphone* Android, dan berdasarkan Tabel 1 dapat dilihat 15

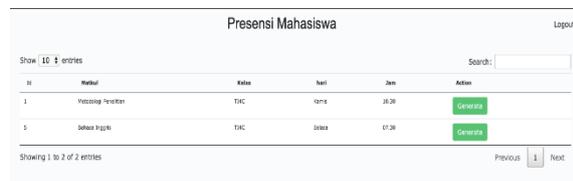
sampel berhasil melakukan fungsi registrasi dengan presentase keberhasilan 100%. Untuk fungsi Identifikasi wajah 14 sampel berhasil melakukan fungsi tersebut dan 1 sampel gagal dengan presentase keberhasilan 93.3%. Untuk fungsi presensi terdapat 14 sampel berhasil melakukan fungsi tersebut dan 1 sampel gagal dengan presentase keberhasilan 93.3%. Grafik hasil pengujian *template matching* dapat dilihat pada Gambar 12. Pengujian *template matching* bertujuan untuk menguji akurasi algoritma untuk mendeteksi wajah pada manusia. Penulis menggunakan 30 sampel dengan perbandingan 15 untuk foto wajah manusia, dan 15 untuk foto bukan wajah manusia. Sampel foto wajah dan bukan wajah manusia dapat dilihat pada Gambar 10. Pengujian dilakukan dengan membandingkan 30 sampel foto dengan *template* gambar yang sudah disediakan. Sampel *template* dapat dilihat pada Gambar 11.



Gambar 5. Halaman Login dan Registrasi



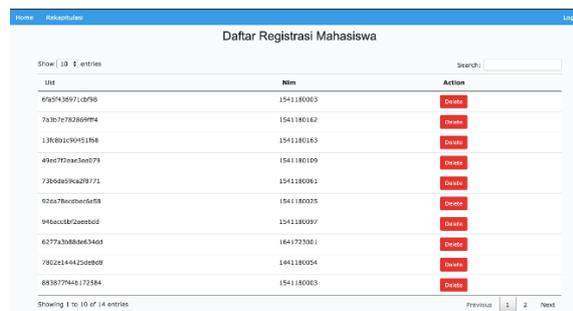
Gambar 4. Activity Diagram pada Sistem



Gambar 6. Halaman Pemilihan Kelas



Gambar 7. Halaman Presensi



Gambar 8. Tampilan Daftar Registrasi Mahasiswa



Gambar 9. Tampilan Rekapitulasi



Gambar 10. Sampel Wajah dan Bukan Wajah



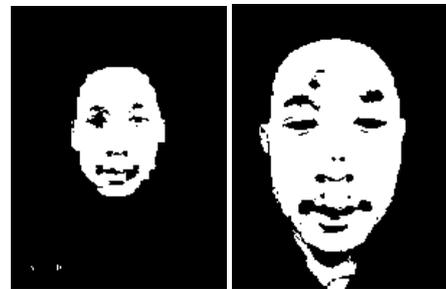
Gambar 11. Penerapan Sistem Absensi

Tabel 1. Pengujian dengan 15 Template

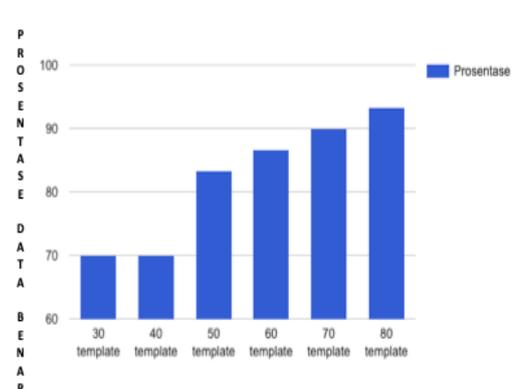
Tabel Pengujian Fungsional					
No	Nim	UID	Regis-trasi	Identi-fikasi Wajah	Pre-sensi
1	1441 1800 54	7802e1 44425d e8d8	berhasil	Berhasil	berhasil
2	1541 1800 03	6fa5f43 6971cbf 98	berhasil	Berhasil	berhasil
3	1541 1801 92	883877 f44b17 2584	berhasil	Berhasil	berhasil
4	1541 1800 25	92da78 ecdbec6 e58	berhasil	Berhasil	berhasil
5	1541 1800 46	b29350 be67f70 13d	berhasil	Berhasil	berhasil
6	1541 1800 61	73b6da 59ca2f8 771	berhasil	Berhasil	berhasil
7	1541 1800 97	946acc 6bf2aee 6dd	berhasil	Berhasil	berhasil
8	1541 1801 09	49ed7f2 eae3ee0 79	berhasil	Berhasil	berhasil
9	1541 1801 60	c9da16 a8e9d9 8757	berhasil	Berhasil	Berhasi l
10	1541 1801 62	7a3b7e 782869 fff4	berhasil	Berhasil	Berhasi l
11	1541 1801 74	df4e9c5 00d258 098	berhasil	Berhasil	Berhasi l
12	1541 1802 30	a0a2cb 2fc73ac 0df	berhasil	Berhasil	Berhasi l

Tabel Pengujian Fungsional					
No	Nim	UID	Regis-trasi	Identi-fikasi Wajah	Pre-sensi
13	1641 7201 13	7ce81b 2e5f716 0f1	berhasil	Gagal	Gagal
14	1641 7201 79	228290 bfe5b12 527	berhasil	Berhasil	Berhasi l
15	1741 7230 15	aeec86c abec42f 44	berhasil	Berhasil	Berhasi l

Template gambar yang digunakan untuk pengujian berjumlah 30, 40, 60, 70, 80 untuk mencari akurasi yang optimal. Pengujian dilakukan tanpa memperhatikan faktor pencahayaan dan jarak foto.



Gambar 12. Face Template



Gambar 12. Pengujian dengan Jumlah Variasi Template

5. Kesimpulan

Dari hasil penelitian penulis berhasil untuk membangun sebuah sistem absensi dengan implementasi metode DS RSA dan Template matching yang terdiri dari berhasil menerapkan algoritma DS RSA pada pembangunan QR Code dan pembacaan QR Code dan juga berhasil menerapkan algoritma Template Matching dalam sistem deteksi wajah. Akurasi tertinggi yang diperoleh dari metode template matching dalam deteksi wajah berdasarkan tes yang dilakukan adalah 93,33% dengan jumlah 80 template wajah, dan akurasi terendah yang diperoleh berdasarkan pengujian adalah 70% dengan jumlah template 30 dan 40 wajah.

Daftar Pustaka:

- Ani, N. et al. (2011): *Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image*, Konferensi Nasional Informatika – KNIF 2011, pp. 148–155.
- Arifin, Z. et al. (2009): *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*, Jurnal Informatika Mulawarman Program Studi Ilmu Komputer Universitas Mulawarman, 4(3), pp. 7–14.
- Bao, F., Lee, C. C. and Hwang, M. S. (2006): *Cryptanalysis and improvement on batch verifying multiple RSA digital signatures*, Applied Mathematics and Computation, 172(2 SPEC. ISS.), pp. 1195–1200. doi: 10.1016/j.amc.2005.03.016.
- Basilio, J. A. M. et al. (2011): *Explicit image detection using YCbCr space color model as skin detection*, Applications of Mathematics and Computer Engineering - American Conference on Applied Mathematics, AMERICAN-MATH'11, 5th WSEAS International Conference on Computer Engineering and Applications, CEA'11, (December), pp. 123–128.
- Çınar Akakin, H. et al. (2006): *2D/3D facial feature extraction*, in Image Processing: Algorithms and Systems, Neural Networks, and Machine Learning. SPIE, p. 60641D. doi: 10.1117/12.643099.
- Dudheria, R. (2018): *Evaluating features and effectiveness of secure QR code scanners*, Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017, 2018-Janua(3), pp. 40–49. doi: 10.1109/CyberC.2017.23.
- Jin, Z. et al. (2007): *Face detection using template matching and skin-color information*, Neurocomputing, 70(4–6), pp. 794–800. doi: 10.1016/j.neucom.2006.10.043.
- Kittur, A. S. and Pais, A. R. (2017): *Batch verification of Digital Signatures: Approaches and challenges*, Journal of Information Security and Applications. Elsevier Ltd, 37, pp. 15–27. doi: 10.1016/j.jisa.2017.09.005.
- Li, Z., Gao, S. and Nai, K. (2017): *Robust object tracking based on adaptive templates matching via the fusion of multiple features*, Journal of Visual Communication and Image Representation, 44, pp. 1–20. doi: 10.1016/j.jvcir.2017.01.012.
- Rochman, F. F., Raharjana, I. K. and Taufik, T. (2017): *Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents*, Scientific Journal of Informatics, 4(1), pp. 8–19. doi: 10.15294/sji.v4i1.7198.
- Thakar, K. et al. (2017): *Implementation and analysis of template matching for image registration on DevKit-8500D*, Optik. Elsevier GmbH, 130, pp. 935–944. doi: 10.1016/j.ijleo.2016.11.057.
- Trivedi, A. K., Thounaojam, D. M. and Pal, S. (2018): *A robust and non-invertible fingerprint template for fingerprint matching system*, Forensic Science International. Elsevier Ireland Ltd, 288, pp. 256–265. doi: 10.1016/j.forsciint.2018.04.045.
- Wijanarko, R. et al. (2017): *Faces detection method based on skin color modeling*, Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017. Elsevier B.V., 4(1), pp. 40–49. doi: 10.1016/j.future.2018.05.082.