Chiffrierte Faksimileübertragung

Autor(en): **Spörndli, J.**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **56 (1983)**

Heft 2

PDF erstellt am: **26.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-561012

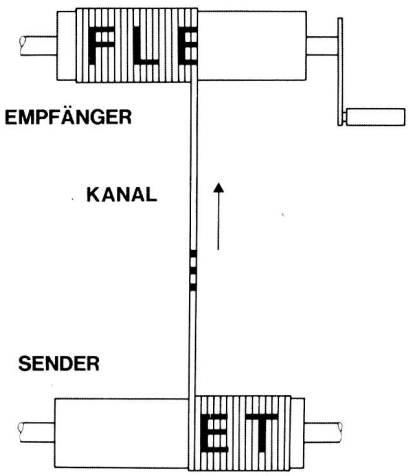
J. Spörndli, El.-Ing. ETH, c/o CRYPTO AG:

Chiffrierte Faksimileübertragung

Digitale Faksimileübertragung ermöglicht das Übertragen von Dokumenten in kurzer Zeit und mit guter Wiedergabequalität. Moderne Faksimilegeräte sind klein, brauchen keine aufwendige Wartung und sind billiger als ihre Vorgänger. Da zudem Bildcodierungs- und Übertragungsverfahren international standardisiert sind, bietet sich die Faksimileübertragung heute als oft sehr viel schnellere Alternative zu den herkömmlichen Mitteln der Dokumentenübertragung an. Im Vordergrund steht die Übermittlung besonders dringender und wichtiger Informationen. Dabei besteht die Notwendigkeit, diese Informationen während der Übertragung schützen zu können. Chiffrierung der Faksimiledaten mit einem geeigneten Zusatz zum Faksimilegerät bietet diesen Schutz auf wirksame Weise ohne Einbusse bezüglich Geschwindigkeit oder Qualität der Übertragung.

Was ist Faksimile-übertragung?

Fax-Übertragung wird durch die deutsche Bezeichnung *Fernkopieren* prägnant beschrieben. Mittels Fax-Übertragung können Dokumente ohne Rücksicht auf ihren Inhalt (Text, Zeichnung, Bild) übermittelt und an einem beliebigen Ort originalgetreu wiedergegeben werden. Fernkopierer unterscheiden sich daher von normalen Bürokopierern vor allem darin, dass sie zwischen Aufnahme und Wiedergabe der Bildinformation die Übertragung über einen *elektrischen Kanal* einfügen:



PRINZIP DER FAKSIMILE-ÜBERTRAGUNG

Bei der Fax-Übertragung wird die Vorlage punkt- und zeilenweise abgetastet, übernommen und wiedergegeben.

- *Aufteilen der Bildinformation* in diskrete Elemente, d.h. zeilenweise Abtastung der Vorlage bei gleichzeitiger Umwandlung der optischen in elektrische Signale.
- *Modulation* der Signale zur Anpassung an den Übertragungskanal.
- *Demodulation,* elektro-optische Umwandlung und zeilenweise Wiedergabe am Empfangsort. («Zeile» steht in diesem Zusammenhang für «Bildzeile»; Dokumente werden typisch mit einer Auflösung von 4–8 Zeilen pro mm abgetastet).

Versuche mit Fax-Übertragung wurden seit der Mitte des 19. Jahrhunderts angestellt. Bis etwa 1960–65 blieben die Anwendungen dieser Technik aber auf wenige Gebiete beschränkt.
Erst in den vergangenen 15–20 Jahren wurde Fernkopieren vor allem dank der immer kürzer werdenden Übertragungszeiten für grössere Anwenderkreise interessant. In der Zeit zwischen 1960 und 1980 vollzog sich für Fax der gleiche Wechsel wie für fast alle Gebiete der Nachrichtentechnik – der Übergang von der Analog- zur Digitaltechnik in der Signalverarbeitung.

Bildabtastung / Wiedergabeverfahren

Erste Fax-Geräte verwendeten rotierende Zylinder als Träger von Vorlage und Kopienpapier, damit sie mit einfachen Abtast/Wiedergabemodulen arbeiten konnten. Diese Verfahren hatten vor allem den Nachteil des hohen Bedienaufwandes und der starken Abnützung der Vorlagen. Die Weiterentwicklung führte deshalb schliesslich zu «Flachbett»-Verfahren, wo die Vorlage auf einer ebenen Unterlage an der Lese- bzw. Schreibeinheit vorbeigeschoben wird. Die Abtast- und Wiedergabevorrichtungen mussten damit komplexer werden, um den Wegfall der Vorlagenrotation zu kompensieren.
Bei der *Abtastung* führte der Weg über Systeme mit beweglichen Lesern und solche mit schwenkbaren Spiegeln hin zur Parallelabtastung ganzer Zeilen durch Photodioden – oder CCD-Zeilen. Dieser letzte Schritt brachte die Aufteilung der Zeilen in Bildpunkte (1 Bildpunkt je Photodiode oder CCD-Zelle) und damit die Digitalisierung im Bereich der Abtastung.
Für die *Wiedergabe* der Bildinformation wurden nach den ersten mechanischen Verfahren der Reihe nach elektrolytische, elektrostatische (allgemein gebräuchlich in Bürokopierern) und schliesslich thermische Aufzeichnungsverfahren angewendet. Die thermische Aufzeichnung arbeitet mit «Thermokämmen», welche zeilenweise schreiben und aus einer gleichen Anzahl Elemente bestehen wie die Abtastzeilen (typischer Wert ist 1728 Elemente bzw. Bildpunkte je Zeile).

Übertragung

Die Bildsignale wurden von den frühen Fax-Geräten zur Übertragung frequenzmoduliert, was Übertragungszeiten von 6 bzw. 4 Minuten (bei reduzierter Vertikalauflösung) pro A4-Seite erlaubte. Um diese Zeiten bei gleichbleibender Auflösung noch weiter verkürzen zu können, wurde dann die einfache Frequenzmodulation durch eine Kombination von Restseitenband-Amplitudenmodulation und Phasenmodulation (VSB-AM/PM) ersetzt, welche eine bessere Ausnützung der verfügbaren Bandbreite brachte. Die Übertragungszeiten fielen so auf 3 bzw. 2 Minuten pro A4-Seite. Mit VSB-AM/PM waren allerdings die Grenzen der Möglichkeiten der Analog-Technik für Fax-Übertragung erreicht.
Um weitere Verbesserungen zu erreichen, musste auf digitale Übertragung der Bildinformation übergegangen werden. Die Bildzeilen werden dabei in einzelne Bildpunkte zerlegt, die Abtastwerte werden quantifiziert (1 Bit zur Aussage «schwarz» oder «weiss») und der entstehende Bitstrom wird mit Hilfe von digitalen Modulatoren/Demodulatoren (Modem) mit einer Datenrate von 4,8 kBit/s übertragen.
Diese Datenrate allein genügt aber nicht, um die bei einer akzeptablen Bildauflösung anfallenden Fax-Daten (2 Millionen Bits pro A4-Seite) in einer genügend kurzen Zeit übertragen zu können. Deshalb wurde zusätzlich *Redundanzreduktion* zur Verringerung der zu übertragenden Datenmenge herangezogen. Die Bildzeilen werden dabei «lauflängencodiert», d.h. es wird jeweils die Anzahl aufeinanderfolgender gleicher Abtastwerte (alle schwarz oder alle weiss) gezählt und diese Zahl durch einen Binärcode ausgedrückt. Durch Übertragen der errechneten Codewörter anstelle der einzelnen Abtastwerte (Bits) resultiert eine Reduktion der Datenmenge um durchschnittlich einen Faktor 10.
Redundanzreduktion und Übertragung mit 4,8 kBit/s erlauben es schliesslich heute, für

eine A4-Seite eine Übertragungszeit von unter einer Minute und eine gute Wiedergabequalität zu erreichen. Natürlich werden weitere Anstrengungen unternommen, um eine zusätzliche Verkürzung der Übertragungszeiten zu erhalten: Einerseits wird versucht, mit zweidimensionaler Codierung die Redundanzreduktion weiter zu erhöhen, andererseits werden die Fax-Modem immer schneller (einzelne Fax-Geräte, welche über gute Verbindungen mit 9,6 kBit/s übertragen können, sind schon heute erhältlich).

Standardisierung der Fax-Geräte

Zu Beginn waren alle Fax-Geräte herstellerspezifisch, d.h., es konnten somit nur Fernkopien zwischen Geräten desselben Herstellers ausgetauscht werden. Dies wirkte natürlich bei Fax besonders störend, weil hier die Übertragung über das grösste öffentliche Netz, das Telefonwählnetz, erfolgt. Der Bedarf für eine Standardisierung war deshalb zwingend; entsprechend formulierte die CCITT verschiedene Empfehlungen für die Fax-Übertragung.

Gruppe 1

Analoggeräte, Bildsignal frequenzmoduliert, Übertragungszeit pro A4-Seite 6 Minuten, Auflösung horizontal etwa 4 Zeilen/mm, vertikal 3,85 Zeilen/mm.

Gruppe 2

Analoggeräte, Modulationsart VSB-AM/PM, Übertragungszeit pro A4-Seite 3 Minuten, Auflösung horizontal etwa 4 Zeilen/mm, vertikal 3,85 Zeilen/mm.

Gruppe 3

Digitalgeräte, Redundanzreduktion mit Lauflängen-Codierung, Modulation nach CCITT V.27ter (Übertragungsrate 4,8 kBit/s), Übertragungszeit pro A4-Seite typisch 40 Sekunden, Auflösung horizontal 8 Bildpunkte/mm, vertikal 3,85 Zeilen/mm.
Zurzeit behandelt CCITT die Empfehlung für die *Gruppe 4;* diese wird die Fax-Übertragung über öffentliche Datennetze spezifizieren.
Die Fax-Geräte, welche heute in der Schweiz eingesetzt werden, verteilen sich wie folgt auf die einzelnen Gruppen:

Etwa 15%
sind Geräte der Gruppe 1. Von diesen entsprechen aber viele nicht genau den Empfehlungen der CCITT, weil diese erst nach den meisten Geräteentwicklungen formuliert wurden.
Kompatibilität zwischen «Gruppe-1-Geräten» ist daher nicht immer gewährleistet. Neue Geräte der Gruppe 1 werden kaum mehr verkauft.

Etwa 70%
sind Geräte der Gruppe 2. Der Telefax-Dienst der Schweizerischen PTT verwendet Geräte dieser Gruppe.

Etwa 15%
sind Digital-Fax-Geräte der Gruppe 3. Viele Geräte verfügen zusätzlich über eine Betriebsart, in der sie auch mit Gruppe-2-Geräten kommunizieren können. Die Zahl der eingesetzten Digitalgeräte wächst am stärksten, weil sie bei sinkenden Preisen höhere Bildqualität und kürzere Übertragungszeit bieten.

Fax-Chiffrierung

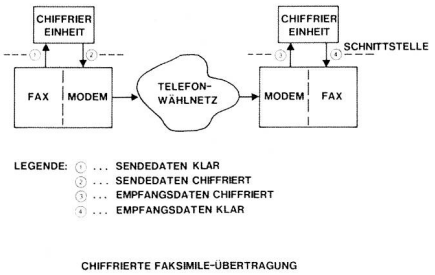
Die Fax-Übertragung wird auch für die Übermittlung von klassifizierten Informationen verwendet. Die Übertragung erfolgt allerdings über das öffentliche Telefonnetz nach einem standardisierten Verfahren; zudem tauschen Gruppe-3-Geräte bei der Verbindungsaufnahme Sender- und Empfängerkennung aus. Dies sind ideale Bedingungen für einen Dritten, welcher die ihn interessierenden Übertragungen mitlesen will. Chiffrierung ist hier das sicherste Mittel, um unbefugtes Mitkopieren zu verhindern.

Chiffrieren von Analog-Fax-Übertragungen

Die bestehenden Chiffriersysteme für Analog-Telefonie sind auf Sprache zugeschnitten. Sie verursachen alle Diskontinuitäten im Zeit- und/oder im Frequenzbereich, welche aber die Sprachqualität nicht wesentlich beeinflussen. Die gleichen Systeme, angewandt auf Fax-Übertragung, würden jedoch keine akzeptable Wiedergabequalität ermöglichen. Fax-Chiffrierung verlangt daher spezielle Techniken. Diese sind zwar heute verfügbar, entsprechende Chiffriergeräte sind im Vergleich zu den Fax-Geräten aber teuer und bieten aufgrund der anzuwendenden Analogverfahren auch nur eine beschränkte Sicherheit.

Chiffrieren von Digital-Fax-Übertragungen

Die Voraussetzungen für das Chiffrieren bei Digital-Fax sind gut; einerseits ist Chiffrieren digitaler Information einfacher als Chiffrieren von Analog-Signalen, andererseits sind die Kosten für die Chiffrierung im Rahmen der Digital-Fax-Systeme besser tragbar.



Prinzipieller Aufbau eines digital-chiffrierten Fax-Systems.

Ein digitales Fax-Gerät enthält eine Schnittstelle, über die beim Sender die unmodulierten Fax-Daten an die Chiffriereinheit und von diesem an das Modem übergeben werden. Beim Fax-Empfänger ist der Datenfluss umgekehrt: Die Daten gehen vom Modem zum Chiffriergerät und von diesem zurück zum Fax-Empfänger. Wichtig ist dabei, dass nur die eigentlichen Bild-Daten, d.h. jene, die mit 4,8 kBit/s übertragen werden, den Chiffrier-/Dechiffrierprozess durchlaufen. Die Initialisierungsdaten, welche von einem zweiten Modem im Fax-Gerät mit 300 Bit/s übertragen werden, bleiben unangetastet.
Auf diese Weise ist die Verbindungsaufnahme mit jedem beliebigen Gruppe-3-Fax-Gerät möglich. Nur wenn sich bei der Initialisierung zeigt, dass beide Fax-Geräte mittels angeschlossenem Chiffriergerät chiffrieren bzw. dechiffrieren können, wird die anschliessende Fax-Übertragung verschlüsselt. Ist dies nicht der Fall, bleibt die Übermittlung der Daten in klar.

Diese Art der Fax-Chiffrierung hat den grossen Vorteil, dass die Kompatibilität des mit einer Chiffriereinheit versehenen Fax-Gerätes in keiner Weise eingeschränkt wird – unverschlüsselter Informationsaustausch ist jederzeit mit jedem andern Gruppe-3-Gerät möglich. Es können aber trotzdem mit den geeigneten Partnerstationen ohne Eingriffe ins System und über den gleichen Telefonanschluss auch verschlüsselte Verbindungen hergestellt werden.
Die *Verschlüsselung* der Fax-Daten wird durch eine bitweise Mischung des Fax-Datenstromes mit einem vom Chiffriergerät erzeugten Pseudozufalls-Bitstrom erreicht. Die Generierung dieses Bitstroms verläuft nach einem komplexen Algorithmus, gesteuert durch den geheimen Schlüssel und einen zufälligen Startzustand. Die Chiffrierung verunmöglicht das Mitlesen der Fax-Daten, sie zerstört jede Struktur im übertragenen, chiffrierten Signal. Die chiffrierten Daten können von einer reinen Zufallsbitfolge nicht unterschieden werden.
Das Chiffrieren/Dechiffrieren der Fax-Daten für die Übertragung wirkt sich in keiner Weise weder auf die Qualität der Fax-Kopie noch auf die Geschwindigkeit der Übertragung aus. Auch bei Übertragungsfehlern entsteht im Vergleich zum unverschlüsselten Betrieb keine Qualitätseinbusse.

Wesentlichste Merkmale des Fernkopierers HF-2060

Abtastverfahren
optoelektronisch mit CCD-Zeile zu 1728 Bildpunkten

Schreibverfahren
thermosensitiv

Übertragung
1. digital mit 4,8 kBit/s und automatischem Fall-Back auf 2,4 kBit/s (bei schlechten Verbindungen)
2. analog mit VSB-AM/PM

Kompatibilität
kompatibel mit allen Fax-Geräten der Gruppen 3 und 2. Die Betriebsart wird bei Verbindungsaufnahme vom Gerät automatisch gewählt.

Empfangsbetrieb
automatisch oder bedient (bedient ist vor allem nötig in den Fällen, wo ein Telefonanschluss nicht ausschliesslich für Fax-Verkehr verwendet werden kann).

Empfangsbestätigung
während der Übertragung wird die Identifikation des Empfängers (Telefonnummer) am sendenden Gerät angezeigt. Nach der Fax-Übertragung teilt das empfangende Gerät dem sendenden mit, ob es die Kopie korrekt erhalten hat oder nicht. Dieser Befund wird wiederum am Sender angezeigt.

CRYPTOFAX HC-440

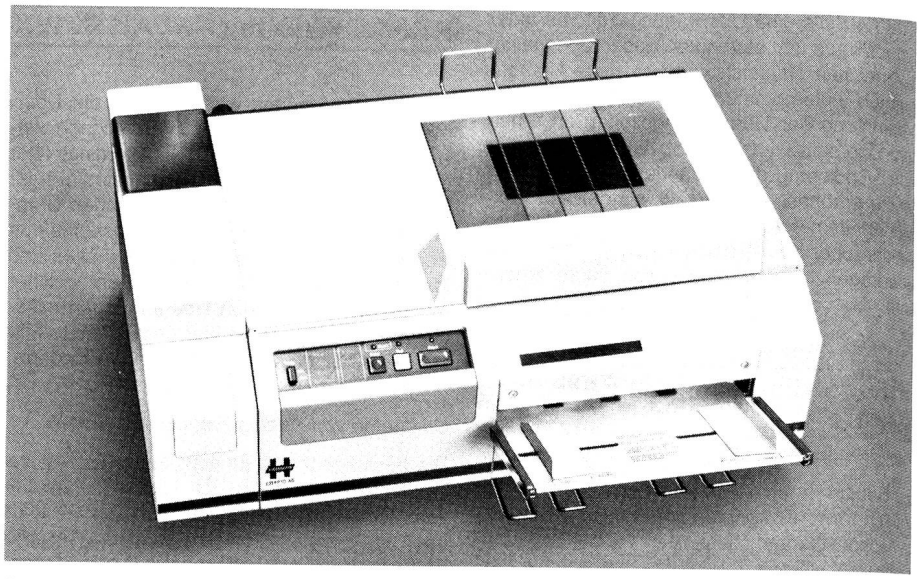
Fernkopierer mit integrierter Chiffrierung

Die Firma CRYPTO AG hat ein Chiffriersystem entwickelt, welches sich generell für die Chiffrierung digitaler Fax-Übertragung eignet (eine Version ist als Zusatz zum Fernkopierer HF-2060 [Siemens] ausgelegt worden). Daraus ergibt sich das kompakte Fax-Chiffrier-System CRYPTOFAX HC-440, das in einem Gehäuse untergebracht werden kann, welches nur wenig

breiter ist als jenes des HF-2060 allein (Gesamtmasse des CRYPTOFAX HC-440: 65×47×28 cm BxTxH).

Die *Merkmale des Chiffriermoduls* sind:

- Die *Vielfalt* des geheimen Schlüssels ist 10^{32} (32 Dezimalziffern, die über eine Tastatur eingegeben werden können). Der Schlüssel bleibt im Gerät permanent gespeichert, kann aber nach der Eingabe nicht mehr gelesen werden.
- Mit dem *Chiffrieralgorithmus* wird vom Schlüssel ein Bitmuster abgeleitet (Periode grösser 10^{15}), welches zur Chiffrierung mit den Fax-Daten verknüpft wird. Durch Wahl eines rein zufälligen Startzustandes wird bei jeder Übertragung ein ganz anderes Bitmuster generiert, wodurch auch bei mehrmaligem Übertragen derselben Vorlage immer verschiedene Chiffratfolgen resultieren.



Das Fax-Chiffriersystem HC-440 setzt sich aus dem Fernkopierer- HF 2060 und dem Chiffriergerät (links aussen) zusammen. *CRYPTOFAX*

- Zur *Synchronisation* von sendender und empfangender Chiffriereinheit wird vor der Übertragung der Fax-Daten jeweils eine Präambel von 500 Bit übermittelt. Die Folge ist eine Verzögerung von 100 bzw. 200 Millisekunden.
- Die *Chiffriereinheit* kann beim Empfang erkennen, ob eine Übertragung chiffriert ist oder nicht und sich entsprechend ein- oder ausschalten. Dies erlaubt unbedienten Empfang von chiffrierten und unchiffrierten Fax-Übertragungen in beliebiger Folge. ●

TELECOMMUNICATIONS CIVILES

Union Internationale des Télécommunications

1983: Année mondiale des communications (II)

P.V. Le précédent article mentionnait l'historique de cette proclamation, le contenu de cette année sur le plan d'organisation, les buts. Il décrivait les projets pilotes planifiés pour la radiodiffusion, la maintenance. Cet article traite des projets en radiocommunication maritime, en gestion et contrôle de fréquences, en propagation, etc.

Radiocommunications maritimes

En Afrique

Toute la côte africaine souffre d'une grave pénurie de bonnes stations de radiocommunications maritimes qui permettraient de *mieux exploiter les transports maritimes et de développer les échanges commerciaux* et, partant, seraient la source de bénéfices considérables. Le projet relatif aux radiocommunications maritimes, exécuté en 1975 et 1976, a quelque peu contribué à définir les besoins et a donné de bons résultats en ce sens que certains pays ont utilisé les spécifications générales établies alors pour acheter du matériel et améliorer leurs installations. Toutefois, depuis 1976, tout le secteur des télécommunications maritimes a connu un révolution avec l'introduction de services par satellites, ainsi que de diverses formes de télégraphie automatique et de traitement des données dans les navires de haute mer. Cependant de nombreux pays africains n'ont même pas des services classiques suffisants pour pourvoir aux besoins du trafic maritime autour de leurs ports et à leur voisinage immédiat. Un effort concerté s'impose si l'on veut que l'Afrique ne perde davantage de terrain dans ce domaine.

Dans les pays de l'ANASE (Indonésie, Malaisie, Philippines, Singapour et Thaïlande)

Les pays de l'ANASE sont largement tributaires des transports et des télécommunicadions maritimes. Les caractéristiques essentielles des délécommunications maritimes font que tous les pays doivent suivre des procédures et des techniques acceptées sur le plan international, afin que les navires de tous les pays puissent communiquer entre eux et avec n'importe quelles stations côtières. La technique des télécommunications maritimes évolue rapidement, en créant de nouveaux services tels que: la télégraphie à impression directe à bande étroite, les communications à courte distance sur ondes métriques et décimétriques, les communications de sécurité, les divers types de radiobalises, l'appel sélectif numérique, l'identification numérique des stations maritimes et l'utilisation de satellites pour les télécommunications maritimes. Ces modifications fondamentales devront être introduites graduellement et efficacement. Il est proposé de fournir les services d'un spécialiste en télécommunications maritimes pour conseiller et assister les pays de l'ANASE dans toutes les questions concernant la mise en place de moyens de radiocommunications suffisants et efficaces pour les stations côtières et les navires de ces pays.

Gestion et contrôle de fréquences en Amérique latine et au Moyen-Orient

Le CCIR, par l'intermédiaire de sa Commission d'études 8, et l'IFRB ont toujours insisté sur la nécessité d'augmenter le nombre de stations